
AccuRoute[®] Embedded Device Client Installation Guide

For AccuRoute v4.1

February 2014



Omttool, Ltd.

6 Riverside Drive
Andover, MA 01810
Phone: +1/1 978 327 5700
Toll-free in the US: +1/1 800 886 7845
Fax: +1/1 978 659 1300

Omttool Europe

25 Southampton Buildings
London
WC2A 1AL
United Kingdom
Phone: +44/0 20 3043 8580
Toll-free in the UK: +44/0 80 0011 2981
Fax: +44/0 20 3043 8581

Web: <http://www.omttool.com>

© 2014 by Omtool, Ltd. All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

Omtool product documentation is provided as part of the licensed product. As such, the documentation is subject to the terms outlined in the End User License Agreement. (You are presented with the End User License Agreement during the product installation. By installing the product, you consent to the terms therein.)

Permission to use the documentation is granted, provided that this copyright notice appears in all copies, use of the documentation is for informational and non-commercial or personal use only and will not be copied or posted on any network computer or broadcast in any media, and no modifications to the documentation are made. Accredited educational institutions may download and reproduce the documentation for distribution in the classroom. Distribution outside the classroom requires express written permission. Use for any other purpose is expressly prohibited by law.

Omtool and/or its suppliers make no guaranties, express or implied, about the information contained in the documentation. Documents and graphics contained therein could include typographical errors and technical inaccuracies. Omtool may make improvements or changes to the documentation and its associated product at any time.

Omtool support and sales

Online resources

The Omtool web site provides you with 24-hour access to documentation, software updates and other downloads, and detailed technical information that can help you troubleshoot issues. Go to <http://www.omtool.com/support> and log in using your customer number. Then click one of the following:

- **Knowledge Base** to access technical articles.
- **Downloads & Docs** to access online documentation, software updates, and downloads.

Customer service and technical support

Contact Omtool Customer Service or Technical Support using any of the following methods:

- **Phone:** +1/1 978 327 6800 or +1/1 888 303 8098 (toll-free in the US)
- **Fax:** +1/1 978 659 1301
- **E-mail:** customerservice@omtool.com or support@omtool.com

Technical support requires an active support contract. For more information, go to <http://www.omtool.com/support/entitlements.cfm>.

Sales, consulting services, licenses, and training

Contact Omtool Sales using any of the following methods:

- **Phone:** +1/1 978 327 5700 or +1/1 800 886 7845 (toll-free in the US)
- **Fax:** +1/1 978 659 1300
- **E-mail:** sales@omtool.com

Contents

Section 1: Introduction

Overview of AccuRoute Embedded Device Client.....	1-1
Main components of the environment.....	1-3
Installation components.....	1-4
Document workflow	1-4
Workflow for the Fax, Routing Sheet, Scan to Destination, and Scan to Distribution features.....	1-5
Workflow for the Fax Release feature	1-6
Workflow for the Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files features.....	1-7
Deploying AccuRoute Embedded Device Client.....	1-8
Basic Requirements.....	1-8
Supported devices.....	1-8
Server requirements	1-9
Device authentication requirements	1-9
Supporting large color documents.....	1-10
Planning for Device Deployment.....	1-11
Configuring to use HTTPS (not supported for HP Pro devices).....	1-11
Custom configuration	1-12
Related documentation.....	1-12

Section 2: Requirements

Supported devices.....	2-1
AccuRoute server requirements	2-3
Device authentication requirements	2-3
Supporting large color documents	2-3
Planning for Device Deployment.....	2-4
Configuring to use HTTPS (not supported for HP Pro devices).....	2-4
Custom configuration	2-4

Section 3: Installation

Installing the AccuRoute Embedded Device Client.....	3-1
Installing the AccuRoute Embedded Device Client on a remote system	3-2

Section 4: Configuring FutureSmart and Oz Devices (only)

Requirements for setting up a CA certificate.....	4-1
Downloading the MakeCert executable	4-2
Creating the certificate	4-2
Installing the certificate to Internet Information Services (IIS).....	4-2
Adding the OPS server certificate to the Client certificate directory.....	4-3
Creating an SSL binding	4-3
Requiring SSL for the virtual web sites	4-4
Verifying the SSL binding	4-4
Enabling directory browsing in IIS.....	4-4
Verifying HTTPS browsing	4-5
Editing the OmISAPIU.xml file	4-5
Editing the Bootstrap.xml file	4-5

Section 5: Configuring HP Pro Devices (only)

Installing the AccuRoute Embedded Device Client on the server	5-1
Installing the OPS kit on the server	5-1
Adding the OPS server certificate to the Client certificate directory.....	5-6
Importing the OPS certificate into the device EWS	5-7
OPS registration	5-7
HTTPS support using the OPS-created certificate.....	5-8
Creating an SSL binding	5-8
Requiring SSL for the virtual web sites	5-8
Verifying the SSL binding	5-8
Enabling directory browsing in IIS.....	5-8
Verifying HTTPS browsing.....	5-9
Editing the OmISAPIU.xml file.....	5-9
Editing the Bootstrap.xml file.....	5-10

Section 6: Configuring Mixed Devices in the Same Environment (HP Pro, FutureSmart, and OZ)

Installing the OPS kit on the server	6-1
Exporting the OPS server certificate from the Trusted Root Certificate Authorities store for HP Pro devices	6-6
Exporting the certificate to the Embedded Device Client directory for FutureSmart and OZ devices	6-7
Importing the OPS certificate into the device EWS	6-7
OPS registration	6-7
HTTPS support for HP Pro devices.....	6-8
Creating an SSL binding	6-8
Requiring SSL for the virtual web sites	6-8
Verifying the SSL binding	6-9
Enabling directory browsing in IIS.....	6-9
Verifying HTTPS browsing.....	6-9
Editing the OmISAPIU.xml file.....	6-10
Editing the Bootstrap.xml file.....	6-10

Section 7: Required Configuration

Adding devices using the AccuRoute Server Administrator	7-1
Creating a group of devices (part 1)	7-1
Creating a group of devices (part 2)	7-6
Updating the Deviceloader.xml to support new devices	7-23
Adding a new device.....	7-23
Choosing an authentication method.....	7-26
Configuring LDAP authentication	7-27
Configuring AccuRoute authentication on the device	7-28
Configuring the server	7-29

Section 8: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

Supported Devices.....	8-1
Exporting the XML files	8-2
Manually importing a certificate.....	8-3
Installing AccuRoute Embedded Device Client buttons	8-5

Section 9: Testing

Testing the Routing Sheet feature.....	9-1
Testing the Device Administrator user interface	9-2

Section 10: Troubleshooting

Detecting workflow issues.....	10-2
Troubleshooting the delivery mechanism	10-2
Troubleshooting messages on the AccuRoute server.....	10-3
Troubleshooting the Web server	10-5
Troubleshooting the multifunction device	10-5
Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd.....	10-5
Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster	10-6
Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet	10-6
Troubleshooting problems associated with applying all additional scan attributes	10-7
Troubleshooting problems when scanning large documents.....	10-7
Troubleshooting problems when scanning 100+ color pages	10-8
Troubleshooting an SNMP error.....	10-9

Appendix A: Configuring HP Pro Devices on a Remote OPS Server with HTTPS Support

Installing the AccuRoute Embedded Device Client on the local server.....	A-1
Installing the OPS kit on the remote server	A-2
Exporting the OPS server certificate.....	A-6
Importing the OPS certificate into the device EWS	A-7
OPS registration	A-7
HTTPS support using the OPS-created certificate.....	A-8

Appendix B: Installing Buttons on HP S900 Series MFP Devices

Adding buttons to HP S900 Series MFP devices.....	B-1
Using Nested buttons	B-2
Device authentication.....	B-3

Section I: Introduction

This guide contains instructions on deploying the AccuRoute Embedded Device Client to multifunction devices. This guide is written for systems administrators with detailed knowledge of the AccuRoute server and the devices. This section of the guide includes:

[Overview of AccuRoute Embedded Device Client](#) (I-1)

[Main components of the environment](#) (I-3)

[Installation components](#) (I-4)

[Document workflow](#) (I-4)

[Deploying AccuRoute Embedded Device Client](#) (I-8)

[Basic Requirements](#) (I-8)

[Planning for Device Deployment](#) (I-11)

[Related documentation](#) (I-12)

Overview of AccuRoute Embedded Device Client

The AccuRoute Embedded Device Client brings the versatile document routing capabilities of AccuRoute to supported devices. These capabilities are founded in Omtool's Distribution Rule technology.

The AccuRoute Embedded Device Client runs on OXP (Open Extensibility Platform), an ASP.NET layer sitting between the device and the AccuRoute server. It communicates between the OXP SDK installed on the device and the AccuRoute server via the Embedded AccuRoute for Intelligent Device Client application.

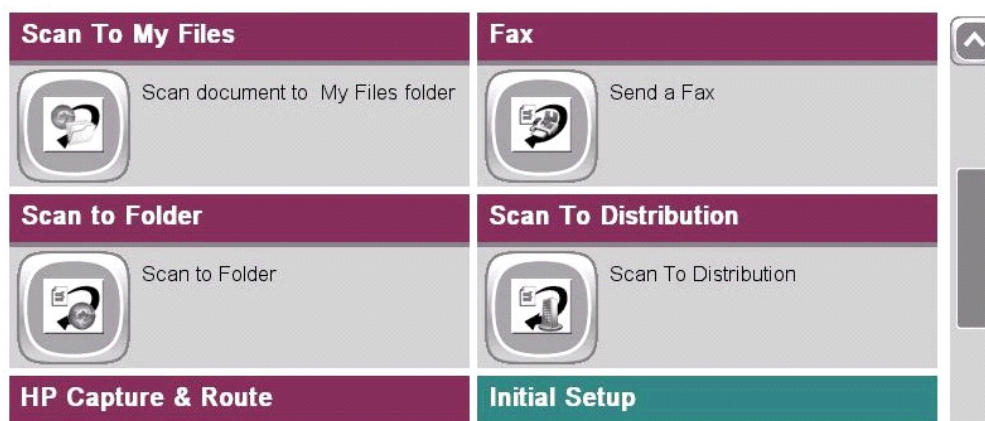


Figure I-1: AccuRoute scanning features on the HP device running AccuRoute Embedded Device Client

Each feature has a unique function that is detailed in the following table. (To see how each feature works on the device, go to [Section 9: Testing](#), for the complete screen sequence of each feature.)

Table I-1: AccuRoute scanning features in AccuRoute Embedded Device Client

Feature	Description	Login required	Notes
Fax	This option allows the user to perform a walk-up fax. The user enters the fax number and can additionally add a cover page to fax. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The AccuRoute server sends the fax to the intended recipients.	No	
Fax Release	This option allows the user to hold or release and print faxes as needed. The user selects the Fax Release button and logs in to the device. Once they enter the Fax number of interest, they can Enable Manual Hold to override the current print schedule, release an existing Manual Hold or Print Pending Jobs (all the faxes currently in queue for the selected fax number).	Yes	The user account associated with this feature must have access to the Administration Node on the Web Client, where they can configure Fax Release Schedule Calendars.
Personal Distributions	The user selects Personal Distributions, logs in to the device, and selects a personal distribution option or Distribution Rule. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server decodes the Distribution Rules and distributes the document to the intended recipient.	Yes	The device user must be able to create Distribution Rules. This requires access to AccuRoute Web Client (where the user can create the Distribution Rules and Routing Sheets).
Public Distributions	The user selects Public Distributions and then selects a public distribution option or Distribution Rule. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server decodes the Distribution Rules and distributes the document to the intended recipient.	No	Public distribution options are associated with a special user account that is set up for this purpose. The user account associated with this feature must be able to create Distribution Rules. This requires access to AccuRoute Web Client (where the user can create the Distribution Rules and Routing Sheets).
Routing Sheet	After the user selects Routing Sheet, the device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server then decodes the Distribution Rule and distributes the document to the intended recipients.	No	The device user must be able to generate Routing Sheets. This requires access to AccuRoute Web Client (where the user can create the Routing Sheets).
Scan to Destination (formerly Scan to Folder; see Notes)	The device scans and delivers the document to the AccuRoute folder via HTTP/HTTPS protocol. The server picks up the scanned document from the network folder, processes it, and delivers it to the intended folder.	No	If you previously used "Scan to Folder" for this button, you must change the display text of the Scan to Destination button. This will be described in Required Configuration (7-1) during the device configuration.
Scan to Distribution	After the user selects Scan to Distribution, the device scans and delivers the documents to a configured distribution.		

Table I-1: AccuRoute scanning features in AccuRoute Embedded Device Client

Feature	Description	Login required	Notes
Scan to Folder	The device scans and delivers the document to a folder (Dropbox, FTP or network folder share) predetermined by your system administrator. The AccuRoute server picks up the scanned document from the network folder, processes it and delivers it to the intended folder.	No	
Scan to Me	The user selects Scan to Me and logs in to the device. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server processes the document using the device user's personal Scan to Me directive and distributes the document to the intended recipients. Or, the scanned document is emailed to the sender (the default).	Yes	Scan to Me is an advanced feature of AccuRoute Web Client. It enables the server to process all AccuRoute messages from the same user with the same Distribution Rule. Scan to Me requires access to AccuRoute Web Client (where the user can create the Distribution Rules and Routing Sheets). In addition, Scan to Me must be configured in the AccuRoute Web Client and on the server. For more information on this feature, consult Section 2: Requirements .
Scan to My Files	The user selects Scan to My Files button and logs in to the device. The device scans and delivers the document to the AccuRoute server (via HTTP/HTTPS protocol) where it is processed and distributed to the My Files section of the user Web Client client.	Yes	All jobs scan.
Mobile Reservations	The user selects the Mobile Reservations button and enters a Mobile Scan Reservation Code generated by the Mobile Client. The device decodes the reservation code and distributes the document to the intended recipients.	No	Mobile Reservations are generated by the Mobile Client and require a Mobile Client license.
Nested Buttons	The Nested Buttons feature provides the ability to configure one top-level button that all other AccuRoute buttons will display under, minimizing the front panel home screen real estate. For example, one button can be configured and labeled "AccuRoute." This button would be the only AccuRoute button to display on the home screen. Pressing this button would then display any other enabled buttons (such as Routing Sheets, Personal Distributions, etc.).	Yes	Login is required only if using Device Authentication and if one of the Nested Buttons needs authentication.

Main components of the environment

The AccuRoute Embedded Device Client environment consists of the following components.

- **AccuRoute Server** - The AccuRoute server is the main back end server for processing and routing documents.

Note AccuRoute v4.0 installs the AccuRoute Intelligent Device Client as part of the server installation. No separate installation of this component is required unless the AccuRoute Embedded Device Client is installed on a remote system, and then the AccuRoute Intelligent Device Client would be installed on the remote system as well.

- **AccuRoute Embedded Device Client** - See [Section 3: Installation](#) for installation instructions.
- **HP Device** - See [Supported devices](#) (2-1) for a list.

Installation components

The AccuRoute Embedded Device Client setup includes multiple components detailed in this table.

Table I-2: Description of installation components with locations and functions

Component	Location	Function
AccuRoute Embedded Device Client Install	...\Omtool\Omtool Server\Clients	The setup contains the setup.exe file for the AccuRoute Embedded Device Client. Use this file to install the AccuRoute Embedded Device Client.
AccuRoute Embedded Device Client Configuration Manager	Devices node in the AccuRoute Server Administrator.	The Device Client Configuration node is a management tool installed with the AccuRoute Server Administrator, and is used to manage settings and options that will be available on the device. Note: A device license must be installed in order for the Device Client Configuration manager node to be used.

Document workflow

The workflow that moves a document from the device to its final destination involves the user, the device, the AccuRoute Embedded Device Client, Embedded AccuRoute for Intelligent Devices (Omtool ISAPI web server extension), and the AccuRoute server. An understanding of this workflow can be helpful in troubleshooting AccuRoute Embedded Device Client integration.

In its most basic workflow, when a device user scans a document, the device submits the document to the AccuRoute Embedded Device Client via HTTP/HTTPS protocol. The AccuRoute Embedded Device Client then routes the document to the AccuRoute server via HTTP/HTTPS protocol. The Dispatch component applies rules to the message and the AccuRoute server processes the message and routes it to the intended recipients.

Workflow for the Fax, Routing Sheet, Scan to Destination, and Scan to Distribution features

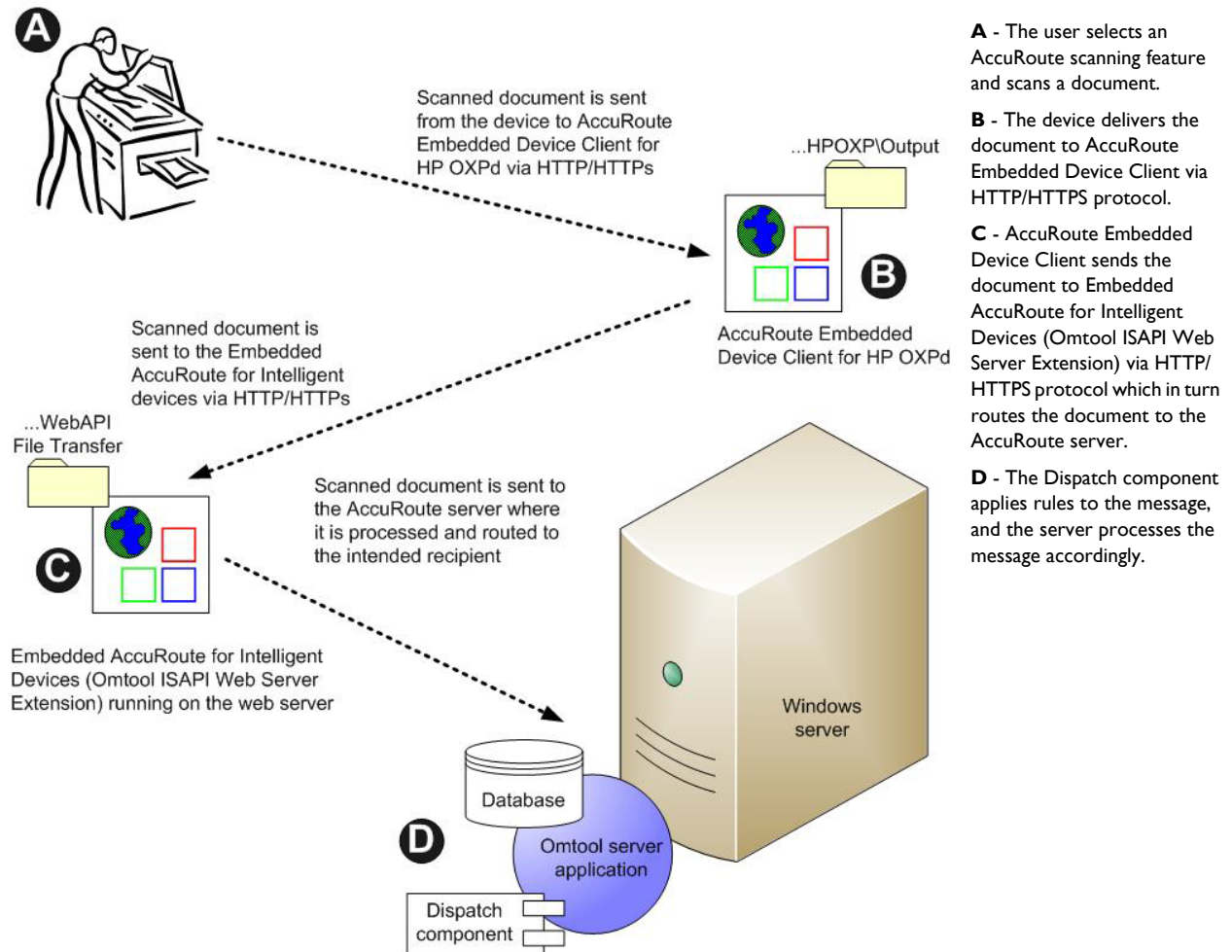


Figure I-2: Workflow for Fax, Routing Sheet, Scan to Destination, and Scan to Distribution

Workflow for the Fax Release feature

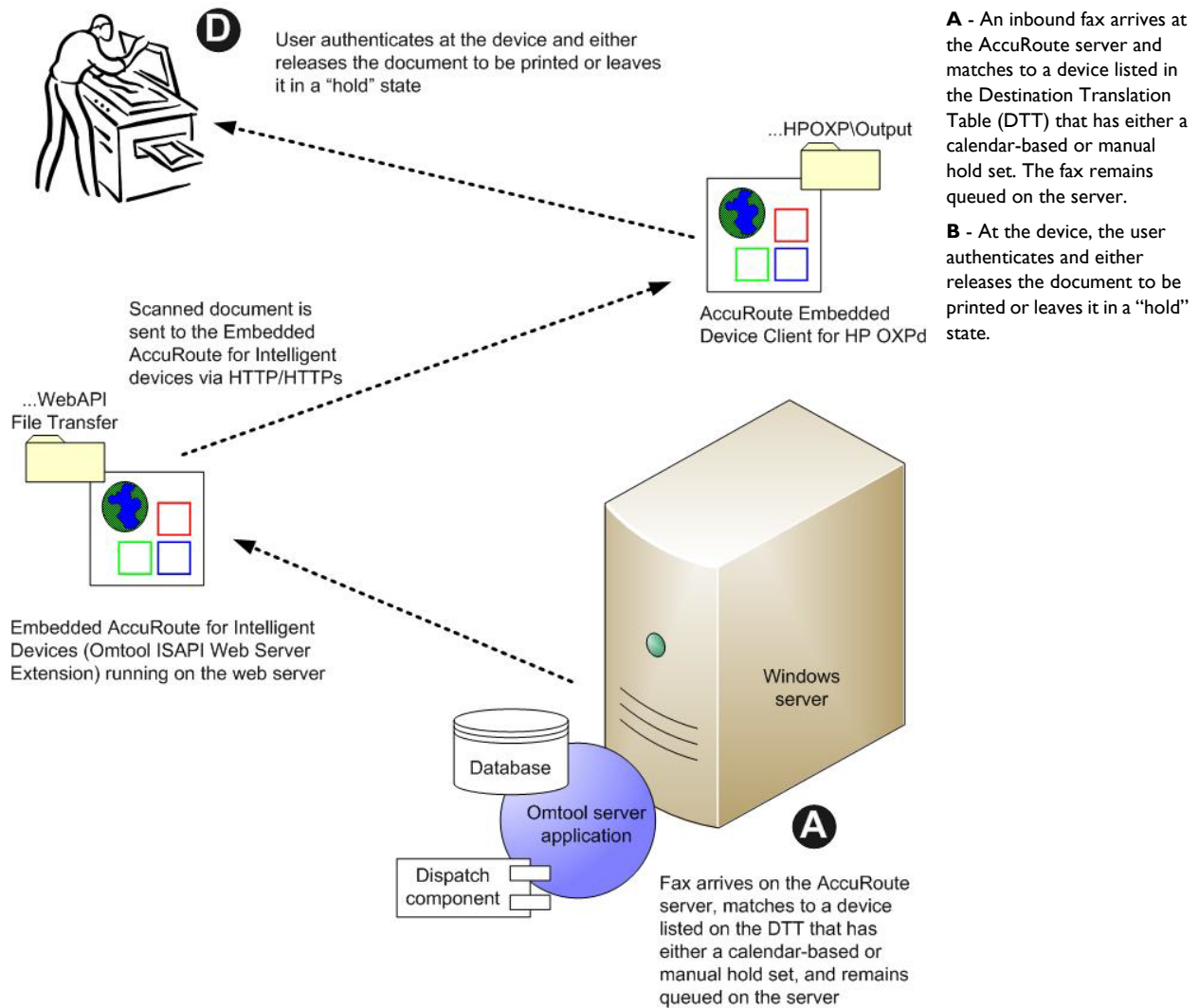


Figure I-3: Workflow for Fax Release

Workflow for the Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files features

When a user begins a scan session with one of these options, the device requests the AccuRoute Embedded Device Client to retrieve Distribution Rules.

Note For Personal Distributions, Scan to Me, and Scan to My Files, the device user must authenticate himself at the device using the configured authentication type. See [Choosing an authentication method \(7-26\)](#).

The AccuRoute Embedded Device Client then submits a request to Embedded AccuRoute for Intelligent Devices (Omtool ISAPI web server extension) which retrieves the data from the AccuRoute server and supplies it to the AccuRoute Embedded Device Client. As soon as the AccuRoute Embedded Device Client returns the data to the device, the workflow resumes.

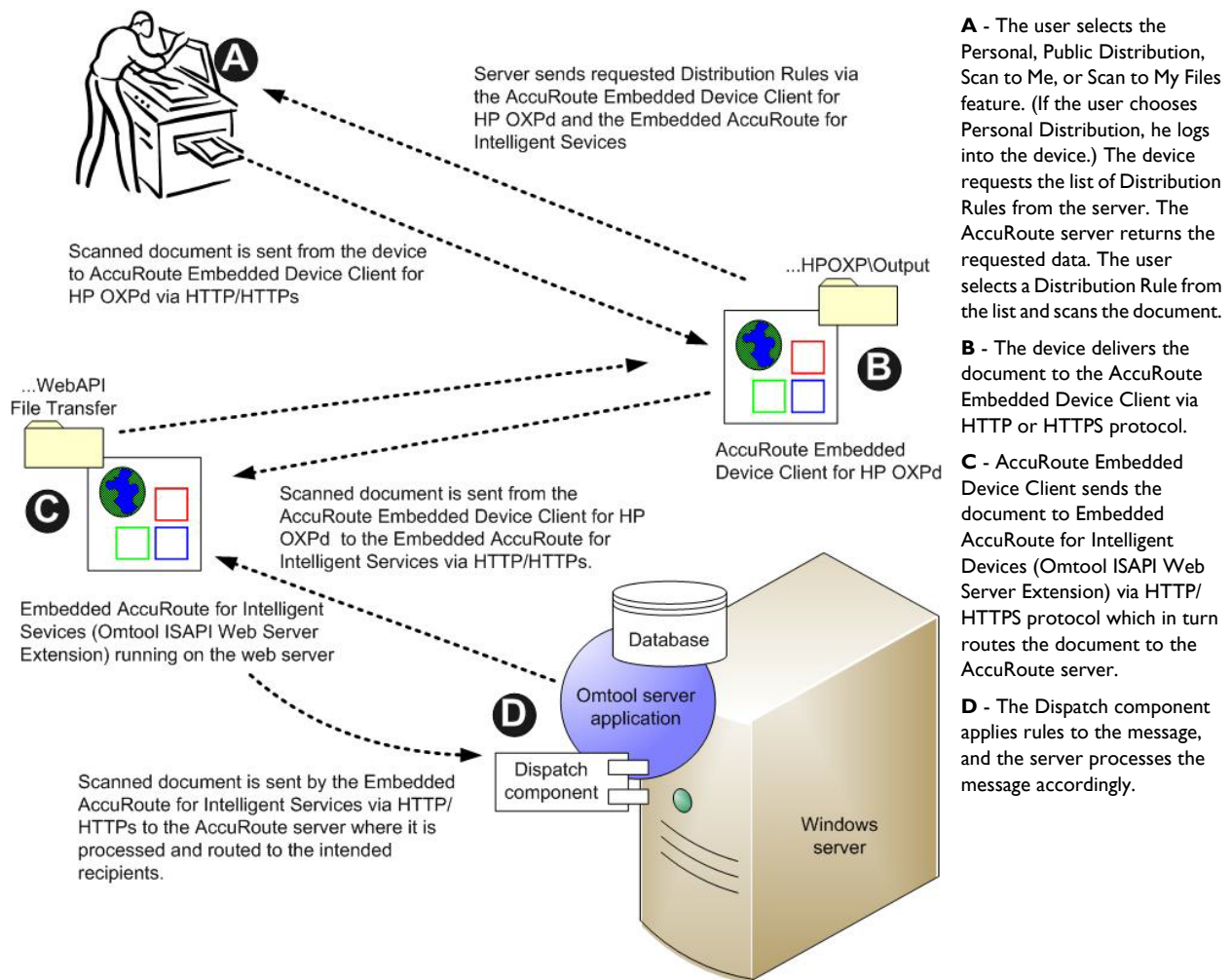


Figure I-4: Workflow for Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files

Deploying AccuRoute Embedded Device Client

- 1 Complete the installation requirements. ([Section 2: Requirements](#))

Note If you are planning to use HTTPS protocol, you must create a CA certificate before installing the AccuRoute Embedded Device Client. Refer to the description of setting up a CA certificate using Microsoft Certificate Services and enabling SSL in [Section 2: Requirements \(2-1\)](#).

- 2 Install the AccuRoute Embedded Device Client. ([Section 3: Installation](#))
- 3 Configure the embedded Web Server of the device. Refer to the description of required configuration in the *AccuRoute® Server Installation and Integration Guide*, which is available through <http://www.omtool.com/documentation/accuroute/4.1/documentation.htm>.
- 4 Configure the AccuRoute server. Refer to the description of configuring the server in the *AccuRoute® Server Installation and Integration Guide*, which is available through <http://www.omtool.com/documentation/accuroute/4.0/documentation.htm>.
- 5 Configure optional capabilities. ([Section 6: Configuring Mixed Devices in the Same Environment \(HP Pro, FutureSmart, and OZ\)](#))
- 6 Test the AccuRoute scanning features on the device. ([Section 9: Testing](#))
- 7 Troubleshoot the setup, if necessary. ([Section 10: Troubleshooting](#))

Basic Requirements

Supported devices

AccuRoute supports the AccuRoute Embedded Device Client on all devices listed in this section.

Table I-3: List of devices supported with the AccuRoute Embedded Device Client

Device	Group	Supported Firmware	OXPD Version
LaserJet M3035 MFP	20	48.250.8	1.6.3.2
LaserJet M4345 MFP	20	48.250.8	1.6.3.2
LaserJet M4349 MFP	20	48.241.2	1.6.3.2
LaserJet M5035 MFP	20	48.283.4	1.6.3.2
LaserJet M5039 MFP	20	48.241.2	1.6.3.2
LaserJet M9040 MFP	20	51.191.3	1.6.3.2
LaserJet M9050 MFP	20	51.191.3	1.6.3.2
LaserJet M9059 MFP	20	51.191.3	1.6.3.2
Color LaserJet CM 4730 MFP	20	50.221.3	1.6.3.2

Table I-3: List of devices supported with the AccuRoute Embedded Device Client

Device	Group	Supported Firmware	OXPd Version
Color LaserJet CM 6030 MFP	40	52.191.2	1.6.3.2
Color LaserJet CM 6040 MFP	40	52.200.4	1.6.3.2
Color LaserJet CM 6049 MFP	40	52.180.5	1.6.3.2
Color LaserJet CM 3530 MFP	50	53.180.3	1.6.3.2
Color LaserJet CM 4540 MFP	XX	2201057_231923	1.6.3.2
ScanJet 7000n	XX	2131311_192131	1.6.3.2
ScanJet 8500	XX	2300293_377163	1.6.3.2
LaserJet Flow M525 MXP	XX	2201074_229181	1.6.3.2
LaserJet Flow M575 MXP	XX	2200893_229649	1.6.3.2
LaserJet M775 MFP	XX	2201057_231933	1.6.3.2
LaserJet M4555 MFP	XX	2200887_229566	1.6.3.2
HP Color LaserJet flow MFP M830	XX	2301122_395323	1.6.3.2
HP Color LaserJet flow MFP M880	XX	2301122_395321	1.6.3.2
HP LaserJet MFP M725	XX	2300312_393688	1.6.3.2
HP Officejet Pro 276dw MFP	XX	FRPICNI336BR	1.6.3.2
HP Officejet Pro x476dn MFP	XX	LNPICA1336CR	1.6.3.2

Note All LaserJet models listed here are part of the *MFP* series. Other LaserJet models that are part of the *printer* series do not have the scanning capabilities required to support the AccuRoute Embedded Device Client.

Note OXPd:SolutionInstaller only supports network-enabled device models. OXPd:SolutionInstaller also requires that the device on which it is running has a writable, non-volatile mass storage partition.

Server requirements

The AccuRoute Embedded Device Client requires:

- AccuRoute Server with appropriate device license
- At least one fax-enabled connector to support fax-based features
- AccuRoute ISAPI Device Client (included with default server install)

Device authentication requirements

The AccuRoute Embedded Device Client supports the following authentication methods. Some of these require setup prior to using the device for scanning. It is recommended that an authentication is selected and verified before installing the device client.

The types of authentication are:

- **Device** authentication uses the native authentication built into the device. This is configurable from the embedded web server.
- **Email** authentication occurs when a user logs into the device with a valid email address that was created in Active Directory.
- **Login** authentication occurs when a users logs into the device with a user name and password as defined in the Active Directory.
- **Pin** authentication displays on the device a text box into which a user enters a PIN login.

Note PIN refers to an attribute of Active Directory and it can be changed to point to any other Active Directory field by modifying the LDAP Lookup Settings Filter field values on the **Authentication** tab of the **Device Group Properties**. The default attribute is set to use **employeeID**.

Note HP Pro Devices do not support the Device authentication method on their own and will require a stacked solution with another authentication service installed. For example: HP AC authentication set in the Pro device when Device authentication is set in AccuRoute.

Supporting large color documents

To support large color documents, you must adjust settings as follows:

- Increase the **Sleep Schedule** from 10 minutes to the maximum, which is 4 hours.
- Increase the **Inactivity Timeout** in the device Embedded Web Server to 300 seconds.
- Increase the **Request Filtering** and **Content Length** values in Internet Information Service Manager (IIS).

Sleep Schedule

To increase the **Sleep Schedule**:

- 1 Log in to the Embedded Web Server on the MFP.
- 2 Select the **General** tab and locate the **Sleep Schedule** section in the left pane.
- 3 Increase the **Sleep Delay** value to the maximum allowable time – 120 minutes.
- 4 Click **Apply**.

Inactivity Timeout

To increase the **Inactivity Timeout** in the device Embedded Web Server:

- 1 Log in to the Embedded Web Server on the MFP.
- 2 Select the **General** tab and locate the **Control Panel Administration** menu.
- 3 Select **Administration** and click **Display Settings**.
- 4 Increase the **Inactivity Timeout** value to 300 seconds.

Request Filtering and Content Length

You need to set the **Request Filtering** value to its maximum of 4294967295. The **Content Length** must be modified on the DeviceClient, OXPd 1.6 and WebAPI sites.

To adjust the **Content Length** and **Request Filtering** settings in IIS:

- 1 Open Internet Information Services (IIS 7) Manager.
- 2 Select **DeviceClient** or **OXPd 1.6** under **Sites**.
- 3 Double-click on **Request Filtering**.
- 4 Select **Edit Feature Settings** under the **Actions** menu.
- 5 Increase the value in **Maximum allowed content length**. The default is 30000000 and it must be increased to [4294967295](#).
- 6 Click **OK**.

Note Repeat steps 2-5 for **WebAPI**.

- 7 Reset IIS.

Planning for Device Deployment

Before you begin installing and configuring your device environment, it is recommended that you review and plan your device configuration. For example, you may want to consider:

- Whether you will group your devices by model, location or functionality.
- If you want to use a Local or Remote IIS server configuration.
- Whether your OPS server is local or remote to your AccuRoute server.

Also, keep in mind that using HP Pro devices in your environment requires an OPS server installation. See [Section 5: Configuring HP Pro Devices \(only\)](#) for more information.

Configuring to use HTTPS (not supported for HP Pro devices)

In order to use HTTPS protocol communication when sending documents from the device to the AccuRoute server, you must create a CA Certificate using Microsoft Certificate Services and enable Secure Socket Layer (SSL). You must create this certificate before installing the AccuRoute Embedded Device Client. This configuration is necessary to allow administrators to export the file and install it on the device to enable HTTPS communication.

Note HTTP and HTTPS cannot coexist and configuration for the device communication must be either HTTP or HTTPS for all devices.

- The administrator will need to create and export the certificate for the Web server as a file named [WebServer.cer](#) and copy it to the Certificate folder created during the AccuRoute Embedded Device Client install.
- During the registration process for the OXPd application onto the device, the [webserver.cer](#) will be installed into the device.

Note No error will be generated if the file does not exist. It will not be possible to configure the device for HTTPS until that file has been installed onto the device.
Also note, if you are using HP Pro devices, the makecert certificates are not supported.

For information on how to create a self-signed certificate using `makecert.exe`, refer to the description of [Creating the certificate](#) (4-2).

Custom configuration

The AccuRoute Server Administrator **Devices** node gives the administrator the ability to manage devices and create groups of devices with customized buttons. Refer to [Creating a group of devices \(part 1\)](#) (7-1).

Related documentation

- [AccuRoute v4.1 Server Installation Guide](#)
- [Omtool Server Administrator Help](#)
- [AccuRoute Embedded Device Client Quick Start Guides](#)

Note The quick start guides have been designed to be posted near the device, distributed to device users, and published on your organization's intranet.

For all documentation related to AccuRoute v4.1, consult the [AccuRoute v4.1 documentation page](#).

Section 2: Requirements

This section includes:

- [Supported devices \(2-1\)](#)
- [AccuRoute server requirements \(2-3\)](#)
- [Device authentication requirements \(2-3\)](#)
- [Supporting large color documents \(2-3\)](#)
- [Planning for Device Deployment \(2-4\)](#)

Supported devices

Omtool supports the AccuRoute Embedded Device Client on all devices listed in this section..

Table 2-1: List of devices supported with AccuRoute Embedded Device Client

Device	Group	Supported firmware	Minimum Installed RAM	OXPd Version	Web Jetadmin (Operation System)
LaserJet M3035 MFP	20	48.250.8	N/A	1.6.3.2	Yes (Oz)
LaserJet M4345 MFP	20	48.250.8	N/A	1.6.3.2	Yes (Oz)
LaserJet M4349 MFP	20	48.241.2	N/A	1.6.3.2	Yes (Oz)
LaserJet M5035 MFP	20	48.283.4	N/A	1.6.3.2	Yes (Oz)
LaserJet M5039 MFP	20	48.241.2	N/A	1.6.3.2	Yes (Oz)
LaserJet M9040 MFP	20	51.191.3	N/A	1.6.3.2	Yes (Oz)
LaserJet M9050 MFP	20	51.191.3	N/A	1.6.3.2	Yes (Oz)
LaserJet M9059 MFP	20	51.191.3	N/A	1.6.3.2	Yes (Oz)
Color LaserJet CM 4730 MFP	20	50.221.3	N/A	1.6.3.2	Yes (Oz)
Color LaserJet CM 6030 MFP	40	52.191.2	N/A	1.6.3.2	Yes (Oz)
Color LaserJet CM 6040 MFP	40	52.200.4	N/A	1.6.3.2	Yes (Oz)
Color LaserJet CM 6049 MFP	40	52.180.5	N/A	1.6.3.2	Yes (Oz)
Color LaserJet CM 3530 MFP	50	53.180.3	N/A	1.6.3.2	Yes (Oz)
Color LaserJet CM 4540 MFP	XX	2201057_231923	N/A	1.6.3.2	Yes (FutureSmart)
ScanJet 7000n	XX	2131311_192131	N/A	1.6.3.2	Yes (FutureSmart)
ScanJet 8500	XX	2300293_377163	N/A	1.6.3.2	Yes (FutureSmart)

Table 2-1: List of devices supported with AccuRoute Embedded Device Client

Device	Group	Supported firmware	Minimum Installed RAM	OXPd Version	Web Jetadmin (Operation System)
LaserJet Flow M525 MXP	XX	2201074_229181	N/A	1.6.3.2a	Yes (FutureSmart)
LaserJet Flow M575 MXP	XX	2200893_229649	N/A	1.6.3.2	Yes (FutureSmart)
LaserJet M775 MFP	XX	2201057_231933	N/A	1.6.3.2	Yes (FutureSmart)
LaserJet M4555 MFP	XX	2200887_229566	N/A	1.6.3.2	Yes (FutureSmart)
HP Color LaserJet flow MFP M830	XX	2301122_395323	N/A	1.6.3.2	N/A
HP Color LaserJet flow MFP M880	XX	2301122_395321	N/A	1.6.3.2	N/A
HP LaserJet MFP M725	XX	2300312_393688	N/A	1.6.3.2	N/A
HP Officejet Pro 276dw MFP	XX	FRPICN1336BR	N/A	1.6.3.2	N/A
HP Officejet Pro x476dn MFP	XX	LNPICA1336CR	N/A	1.6.3.2	N/A

Note All LaserJet models listed here are part of the *MFP series*. Other LaserJet models that are part of the *printer series* do not have the scanning capabilities required to support the AccuRoute Embedded Device Client.

Note OXPd:SolutionInstaller only supports network-enabled device models.
 OXPd:SolutionInstaller also requires that the device on which it is running has a writable, non-volatile mass storage partition.

AccuRoute server requirements

The AccuRoute Embedded Device Client requires:

- AccuRoute server v4.1
 - ▶ with appropriate license
 - ▶ fax-enabled to support fax-based features
- At least one fax-enabled connector to support fax-based features
- AccuRoute ISAPI Device Client (included with default server install)
- ASP.NET 3.5.1

Device authentication requirements

The AccuRoute Embedded Device Client supports the following authentication methods. Some of these require setup prior to using the device for scanning. It is recommended that an authentication is selected and verified before installing the device client. See the *AccuRoute v4.1 Server Installation Guide* ([AccuRoute v4.1 documentation page](#)).

The types of authentication are:

- **Device** authentication uses the native HP authentication built into the device. This is configurable from the Embedded Web Server.
- **Email** authentication occurs when a user logs into the device with a valid email address that was created in Active Directory.
- **Login** authentication occurs when a user logs into the device with a user name and password as defined in the Active Directory.
- **Pin** authentication displays on the device a text box into which a user enters a PIN login.

Note PIN refers to an attribute of Active Directory and it can be changed to point to any other Active Directory field by modifying the LDAP Lookup Settings Filter field values on the **Authentication** tab of the **Device Group Properties**. The default attribute is set to use **employeeID**.

Note HP Pro Devices do not support the Device authentication method on their own and will require a stacked solution with another authentication service installed. For example: HP AC authentication set in the Pro device when Device authentication is set in AccuRoute.

Supporting large color documents

To support large color documents, an IIS setting (Request Filtering) must be set to the maximum 4294967295. Content length must be modified on the WebAPI site. To increase content length in IIS:

- 1 Open Internet Information Services (IIS 7) Manager.
- 2 Select **WebAPI** under **Sites**.
- 3 Double-click on **Request Filtering**.
- 4 Select **Edit Feature Settings** under the **Actions** menu.
- 5 Increase the value in **Maximum allowed content length**. The default is 30000000 and it must be increased to **4294967295**.
- 6 Reset IIS.

Planning for Device Deployment

Before you begin installing and configuring your device environment, it is recommended that you review and plan your device configuration. For example, you may want to consider:

- Whether you will group your devices by model, location or functionality.
- If you want to use a Local or Remote IIS server configuration.
- Whether your OPS server is local or remote to your AccuRoute server.

Also, keep in mind that using HP Pro devices in your environment requires an OPS server installation. See [Configuring HP Pro Devices \(only\)](#) (19) for more information.

Configuring to use HTTPS (not supported for HP Pro devices)

In order to use HTTPS protocol communication when sending documents from the device to the AccuRoute server, you must create a CA Certificate using Microsoft Certificate Services and enable Secure Socket Layer (SSL). You must create this certificate before installing the AccuRoute Embedded Device Client. This configuration is necessary to allow administrators to export the file and install it on the device to enable HTTPS communication.

Note HTTP and HTTPS cannot coexist and configuration for the device communication must be either HTTP or HTTPS for all devices.

- The administrator will need to create and export the certificate for the Web server as a file named “WebServer.cer” and copy it to the Certificate folder created during the AccuRoute Embedded Device Client install.
- During the registration process for the OXPd application onto the device, the webserver.cer will be installed into the device.I0

Note No error will be generated if the file does not exist. It will not be possible to configure the device for HTTPS until that file has been installed onto the device.
Also note, if you are using HP Pro devices, the makecert certificates are not supported.

For information on how to create a self-signed certificate using makecert.exe, refer to the description of [Creating the certificate](#) (14).

Custom configuration

The AccuRoute Server Administrator Devices node gives the administrator the ability to manage devices and create groups of devices with customized buttons. Refer to [Creating a group of devices \(part 1\)](#) (39).

Section 3: Installation

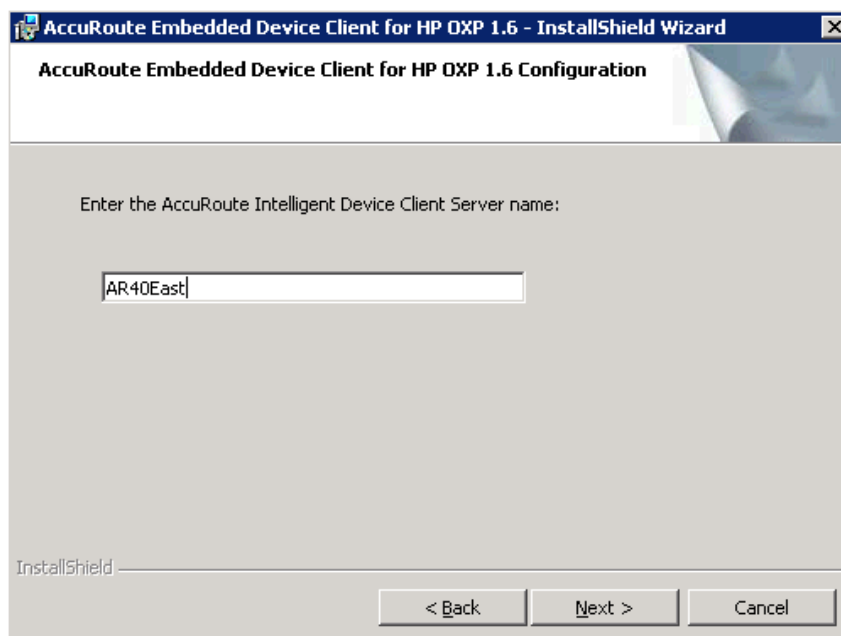
This section includes:

[Installing the AccuRoute Embedded Device Client](#) (3-1)

[Installing the AccuRoute Embedded Device Client on a remote system](#) (3-2)

Installing the AccuRoute Embedded Device Client

- 1 Log on to the system running the AccuRoute server using an account that belongs to the local Administrators group.
- 2 Navigate to the folder `C:\Program Files (x86)\Omtool\Omtool Server\Clients\DeviceClient` and run `setup.exe`.
The InstallShield wizard launches with the **Welcome** message.
- 3 Click **Next**. The **Destination Folder** page opens.
- 4 Keep the default location and click **Next**. The **AccuRoute Embedded Device Client Configuration** page opens.



- 5 In the **AccuRoute Intelligent Device Client Server name** text box, enter the AccuRoute server name or the IP address of the AccuRoute Intelligent Device Client.
- 6 Click **Next** and you are ready to install the program.

- 7 Click **Install** to begin installation. The setup installs AccuRoute Embedded Device Client. The InstallShield Wizard shows a message indicating when the installation is complete.
- 8 Click **Finish**.
- 9 Continue to [Section 7: Required Configuration](#).

Installing the AccuRoute Embedded Device Client on a remote system

- 1 Log on to the system where you want to install the AccuRoute Embedded Device Client using an account that belongs to the local Administrators group.

Note The system must be running Windows 2008 R2 or 2012 64-bit and must have Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) and AccuRoute v4.1 installed.

- 2 Navigate to the `\\Omtool\Omtool Server\Clients\DeviceClient` directory and run `setup.exe`.
The InstallShield wizard configures your system for installation and shows the **Welcome** message.
- 3 Click **Next**. The **AccuRoute Embedded Device Client Configuration** page opens.
- 4 In the **AccuRoute Intelligent Device Client Server name** text box, enter the AccuRoute server name or the IP address of the AccuRoute Intelligent Device Client.
- 5 Click **Next**.
- 6 Click **Install** to begin installation. The setup installs AccuRoute Embedded Device Client. The InstallShield Wizard shows a message indicating when the installation is complete.
- 7 Click **Finish**.
- 8 Continue to [Section 7: Required Configuration](#).

Section 4: Configuring FutureSmart and Oz Devices (only)

This section describes the configuration process for FutureSmart and OZ devices only. The configuration consists of setting up a CA certificate using Microsoft Certificate Services and enabling SSL.

Note If you are using HTTP, skip this section and go to [Section 6: Required Configuration \(6-41\)](#).

If you require HTTPS support, you can follow the instructions in this section to set up a CA certificate with the Microsoft Certificate Services and enable SSL.

Otherwise, use a certificate from a trusted certificate authority. The certificate must be installed on the IIS system.

Note The CA Certificate steps in this section are not supported for HP Pro devices.

Requirements for setting up a CA certificate

You must meet the following requirements when setting up a CA certificate:

- Web server that meets the requirements for AccuRoute Intelligent Device Client.
- Windows user account that belongs to the Administrators group.

The remainder of this section provides procedures for:

[Downloading the MakeCert executable \(4-2\)](#)

[Creating the certificate \(4-2\)](#)

[Installing the certificate to Internet Information Services \(IIS\) \(4-2\)](#)

[Adding the OPS server certificate to the Client certificate directory \(4-3\)](#)

[Creating an SSL binding \(4-3\)](#)

[Requiring SSL for the virtual web sites \(4-4\)](#)

[Verifying the SSL binding \(4-4\)](#)

[Enabling directory browsing in IIS \(4-4\)](#)

[Verifying HTTPS browsing \(4-5\)](#)

[Editing the OmISAPIU.xml file \(4-5\)](#)

[Editing the Bootstrap.xml file \(4-5\)](#)

You should complete each procedure in the order in which they are presented.

Downloading the MakeCert executable

Copy `makecert.exe` to your local computer. The MakeCert executable is available as part of the Windows SDK. For instructions on how to download the Windows SDK and the MakeCert executable, see the [Microsoft documentation](#).

When the download is complete, copy the executable to a shared network folder from where you can access it.

Creating the certificate

- 1 Open a command prompt and navigate to the directory where you saved the MakeCert executable (`makecert.exe`) on your local computer (typically on the C drive).
- 2 Run the following command (as Administrator):

```
makecert.exe -r -pe -n "CN=fully_qualified_domain_name_of_iis_server" -b
01/01/2006 -e 01/01/2013 -ss my -sr localMachine -sky exchange -sp
"Microsoft RSA SChannel Cryptographic Provider" -sy 12
"fully_qualified_domain_name_of_iis_server.cer"
```

fully_qualified_domain_name_of_iis_server should be in this format:
`servername.domain.com`

Note You cannot copy and paste the command text above due to formatting issues. This text is available to copy in the AccuRoute Embedded Device Client section of the [On-line help for the administrator](#). If you key in the command text, note that there is a space at the end of the first three lines shown above.

When the command is run properly, the system will display a message indicating that it succeeded.

Installing the certificate to Internet Information Services (IIS)

You must now install the certificate from the root of C.

- 1 Select and right-click the certificate.
- 2 Select **Install Certificate**. The **Certificate Import** wizard appears.

Note In Windows 2012 environments, the **Certificate Import Wizard** prompts you to select either **Current User** or **Local Machine**. Select **Local Machine**.

- 3 Select **NEXT**.
- 4 Select **Place all certificates in the following store** and select **BROWSE**.

- 5 Select **Trusted Root Certification Authorities** and select **OK**.
- 6 You will be prompted with a security warning:
You are about to install a certificate from a certification authority (CA) claiming to represent...
Do you want to install this certificate?
Select **YES**. A message indicating the import was successful should appear.

Adding the OPS server certificate to the Client certificate directory

- 1 Navigate to the `IIS\LOCAL MACHINE` directory and locate **Server Certificates**.
- 2 Locate the newly created certificate. Double-click to open the certificate **Properties** page.
- 3 Click on the **Details** tab.
- 4 Choose the **Copy to File** option. The **Certificate Export** wizard opens.
- 5 Click **Next**.
- 6 In the **Export Private Key** dialog, select **No, do not export the private key**.
- 7 Click **Next**.
- 8 In the **Export File Format** dialog, select **DER encoded binary X.509 (.CER)**.
- 9 Click **Next**.
- 10 In the **File to Export** dialog, select **Browse**. The **Save As** dialog opens.
- 11 Browse to the directory:
`C:\Program Files (86)\Omtool\DeviceClient\Certificate`
- 12 In the **File Name** field, enter **WebServer.cer with DER Encoded Binary X.509 (*.cer)** as the **Save Type**.
- 13 Click **Save** and then **Next**. The **Completing the Certificate Export** wizard opens.
- 14 Click **Finish**.
- 15 When a message appears stating that the export was successful, click **OK**.

Creating an SSL binding

- 1 Open the IIS Manager.
- 2 Click on the **Default Web Site** and locate **Bindings** under **Edit Site** (top right corner of the window).
- 3 Click on **Bindings**. The **Site Bindings** dialog opens.
- 4 Click on **HTTPS type** and select **Edit**. The **Edit Site Bindings** dialog opens.

- 5 In the **SSL certificate** drop-down, choose the certificate that was created earlier and click **OK**.
- 6 Click **Close** to close the dialog.

Requiring SSL for the virtual web sites

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **Device Client**.
- 3 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.
- 4 Expand **Local machine > Default Web Site** and select **WebAPI**.
- 5 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.

Verifying the SSL binding

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 3 Click on **Browse *:443 (HTTPS)** under **Manage Application/Browse Application** (located at the top right corner of the IIS dialog).

You will see this message: *There is a problem with this web site's security certificate.*

Note This message is expected and safe to ignore.

- 4 Click the **Continue to this website (not recommended)** option.
- 5 Verify that the **IIS 7** dialog opens.

Enabling directory browsing in IIS

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **DeviceClient**.
- 3 Double-click on **Directory browsing**.
- 4 In the right **Actions** field, select **ENABLE**.
- 5 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 6 Double-click on **Directory browsing**.
- 7 In the right **Actions** field, select **ENABLE**.

Verifying HTTPS browsing

- 1 Open the IIS Manager.
- 2 Expand the **Default Web Site**.
- 3 Expand **OXP**.
- 4 Select the **Configuration** folder.
- 5 In the actions pane, select **Browse*:443(https)**.
- 6 Select **Continue to this website (not recommended)**.
- 7 Verify that the local page is displayed:
`.../DeviceClient/Configuration/`
- 8 In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
- 9 In the actions pane, select **Browse*:443(https)**.
- 10 Select **Continue to this website (not recommended)**.
- 11 Verify that the localhost page is displayed:
`.../WebAPI/`
- 12 Select **Continue to this website (not recommended)**.

Editing the OmISAPIU.xml file

- 1 Navigate to the following path.
`C:\Program Files (x86)\Omtool\Omtool Server\WebAPI\WebAPI\Scripts`
- 2 In OmISAPIU.xml, find the FileTransfer node. Replace the IP address with the fully qualified domain name. Also, change `http` to `https`.

```
<FileTransfer>https://fully_qualified_domain_name/WebAPI/FileTransfer/  
</FileTransfer>
```

Note XML files can be edited using Microsoft Notepad.

- 3 Save the file.

Editing the Bootstrap.xml file

- 1 Navigate to the following path.
`C:\Program Files (x86)\Omtool\DeviceClient\Configuration`
- 2 In bootstrap.xml, change `http` to `https`.

```
<Server>https://fully_qualified_domain_name/webapi/scripts/omisapiu.dll  
</Server>
```

- 3** Save the file.
- 4** Reset IIS.

Section 5: Configuring HP Pro Devices (only)

This section describes the installation and configuration process for local HP Pro devices only.

HP Pro devices require an OPS server for registration prior to installing feature buttons on the devices. The OPS server creates a certificate used for a secure registration of each Pro device. You can also use this certificate in your IIS server for HTTPS support.

The OPS Server installation process includes the following steps:

[Installing the AccuRoute Embedded Device Client on the server](#) (5-1)

[Installing the OPS kit on the server](#) (5-1)

[Adding the OPS server certificate to the Client certificate directory](#) (5-6)

[Importing the OPS certificate into the device EWS](#) (5-7)

[OPS registration](#) (5-7)

[HTTPS support using the OPS-created certificate](#) (5-8)

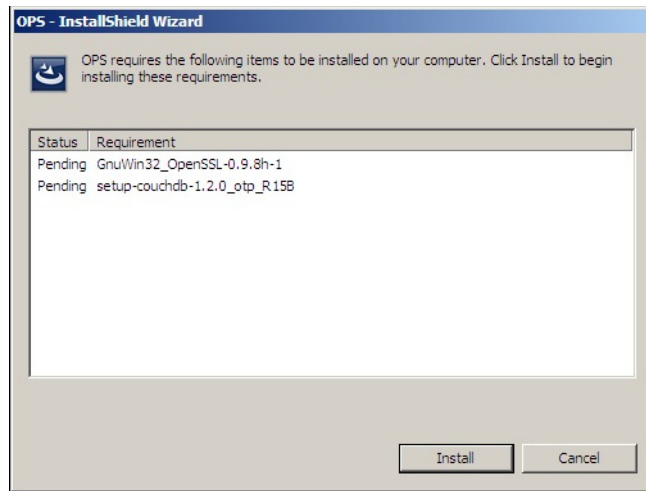
Installing the AccuRoute Embedded Device Client on the server

On the system running the AccuRoute server, install the AccuRoute Embedded Device Client. See [Installing the AccuRoute Embedded Device Client](#) (3-1) for more information.

Installing the OPS kit on the server

- 1 On the server, navigate to `C:\Program Files (x86)\Omtool\Omtool Server\Tools`.
- 2 Right-click and select **Run as Administrator**.
- 3 Run `setup.exe` for OPS.
- 4 The OPS InstallShield wizard appears and requests that you install the following two items:
 - ▶ `GnuWin32_OpenSSL-0.9.8h-1`
 - ▶ `setup-couchdb-1.2.0_otp_R15B`

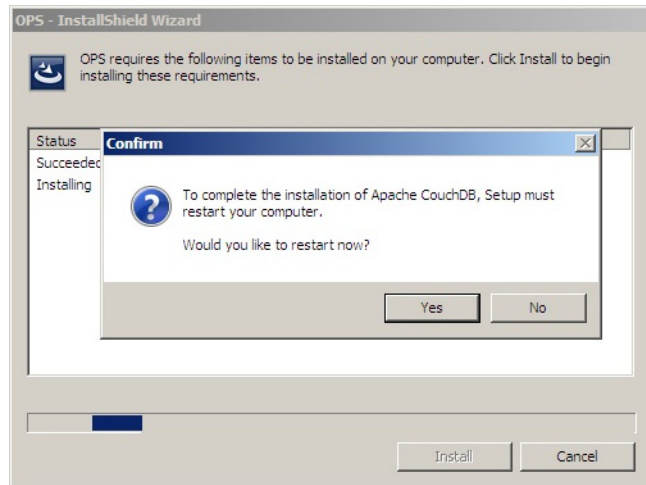
Section 5: Configuring HP Pro Devices (only)



5 Click **Install**.

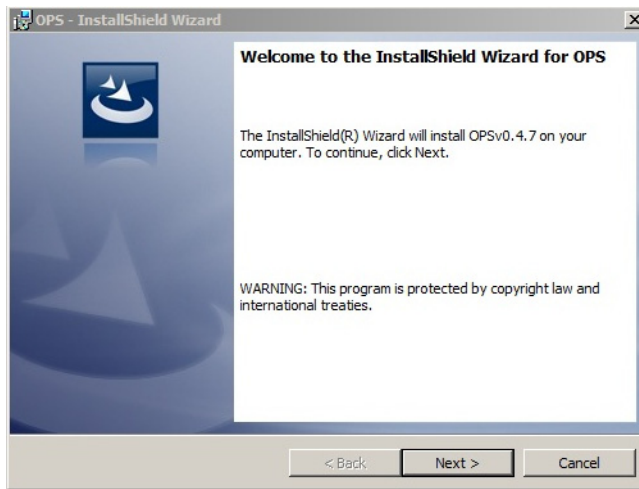
6 After installing the items in Step 3, the following message may appear:

To complete the installation of Apache CouchDB, setup must restart your computer. Would you like to restart now?



If this message appears, click **Yes** to restart. The OPS InstallShield wizard reappears upon restarting the system.

Otherwise, the OPS InstallShield wizard **Welcome** screen immediately appears.

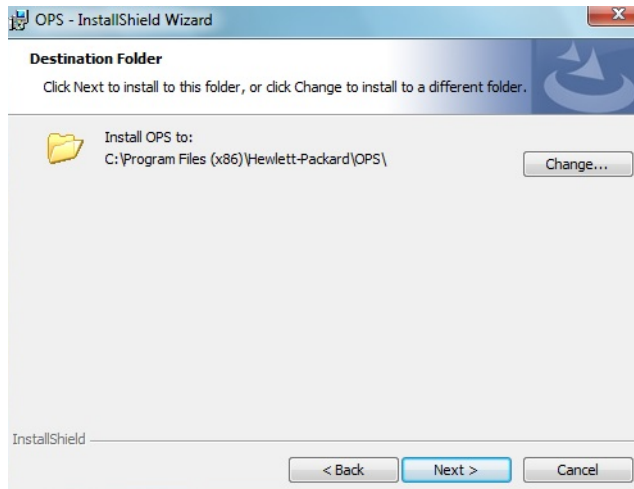


7 Click **Next**. The **License Agreement** screen appears.

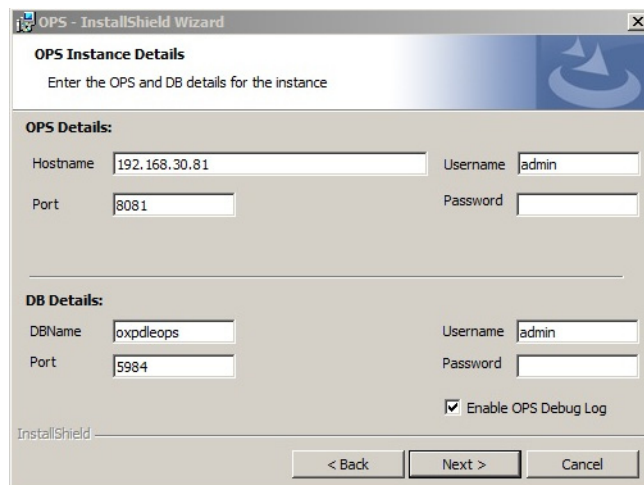


8 Select **I accept the terms in the license agreement** and click **Next**.

The **Destination Folder** screen appears.

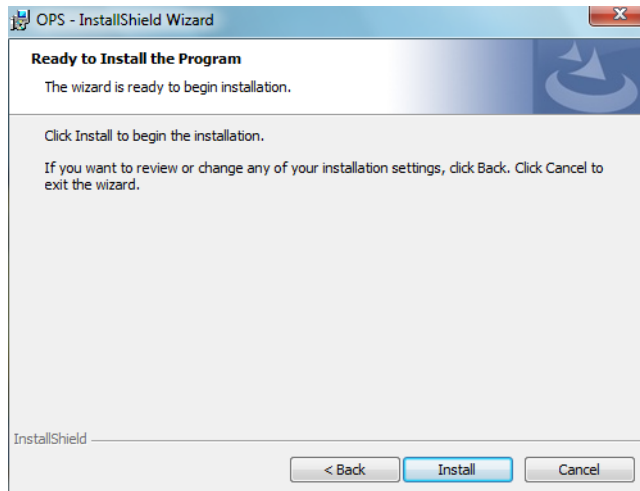


9 Click **Next**. The **OPS Instance Details** screen appears.



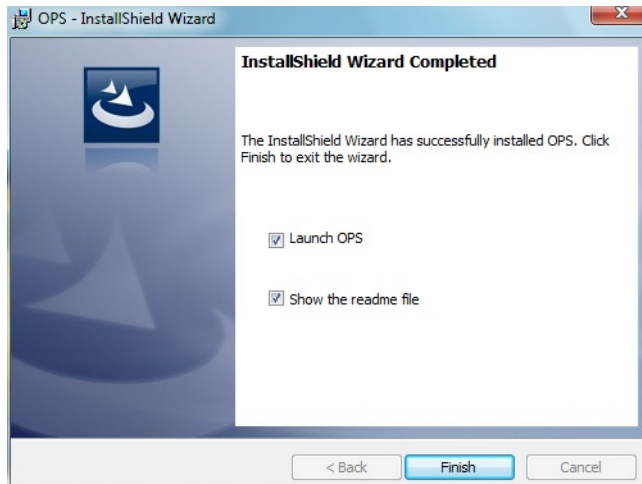
- 10** In the **Hostname** field enter either the IP or FQDN of the server on which OPS is installed. This value is the OPS server name. Make note of this value, as you will need to reference it later during device registration and HTTPS configuration.
- 11** Enter the **Passwords** in both the **OPS Details** and **DB Details** sections. Also make note of these for later use.

12 Click Next.The **Ready to Install the Program** screen appears.



13 Click Install.

14 The OPS InstallShield Wizard Completed screen appears.

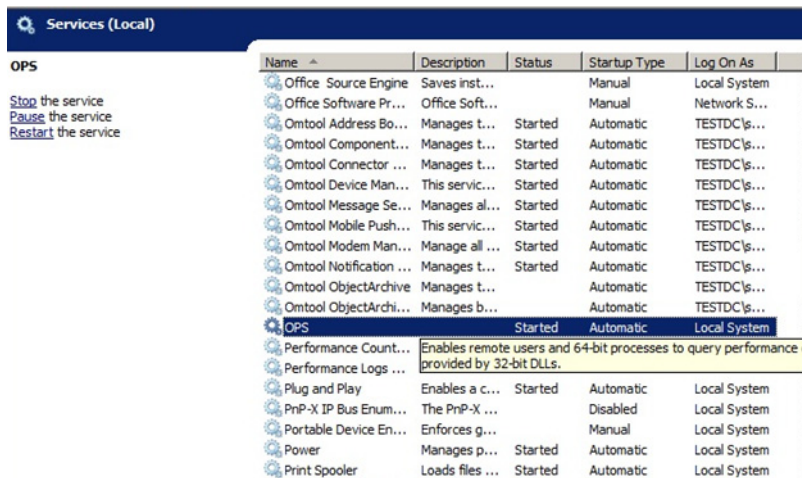


Select both the **Launch OPS** and **Show the readme file** check boxes (**Show the readme file** is optional) and then click **Finish**.

A pop-up message appears to inform you that the OPS server is listening at the IP address and port listed in step 9.



Click **OK**. OPS now appears as a Windows service.



Adding the OPS server certificate to the Client certificate directory

- 1 Open a Windows console and select **File > Add /Remove snap in...**
- 2 Select **Certificates** and click the **Add** button. The **Certificates snap-in** wizard appears.
- 3 Select the **Computer account** radio button and click **Next, Finish** and **OK**.
The console loads with the new Certificate snap-in.
- 4 Expand **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.

- 5 Right-click the **OPS certificate** and select **All tasks > Export**.
- 6 The **Certificate Export** wizard appears. Select **Next**.
- 7 Choose **Base-64 encoded x.509(.CER)** and select **Next**.
- 8 Name the file and select **Browse**.
- 9 Place the certificate in `C:\Program Files (x86)\Hewlett-Packard\OPS`.
- 10 Select **Next** and then click **Finish**.

Importing the OPS certificate into the device EWS

- 1 Open and log into the EWS of the Pro Device.
- 2 On the **Network** tab select **Advanced settings > Certificates**.
- 3 Select **Import > Choose File**.
- 4 Browse to the location where the OPS certificate was saved and select **Open** and then **Finish**.

OPS registration

- 1 At a command prompt enter

```
C:\Program Files (x86)\Hewlett-Packard\OPS\bin>OPSSetup
```
- 2 You will be prompted to choose from a selection of options.
Select **Option 3: Register a device to the OPS server**.
- 3 Enter the IP address for the device. For example, `123.456.78.9`.
- 4 Enter the device **username** and **password** you want to use, noted from [Installing the OPS kit on the server](#) (5-1).
- 5 Enter the **OPS server URL** you want to register. For example, `https://<hostname or IP>:port`.
- 6 Enter the **username** and **password** for the OPS server.

Note The OPS server URL and username can be obtained from Steps 8 and 9 above in [Installing the OPS kit on the server](#) (5-1).

- 7 The following message appears:

```
OPS Registered successfully
```

Your local OPS server is now installed. See [Creating a group of devices \(part I\)](#) (6-41) for more information on creating device groups.

HTTPS support using the OPS-created certificate

Creating an SSL binding

- 1 Open the IIS Manager.
- 2 Click on the **Default Web Site** and locate **Bindings** under **Edit Site** (top right corner of the window).
- 3 Click on **Bindings**. The **Site Bindings** dialog opens.
- 4 Click on **HTTPS type** and select **Edit**. The **Edit Site Bindings** dialog opens.
- 5 In the **SSL certificate** drop-down, choose the certificate that was created earlier and click **OK**.
- 6 Click **Close** to close the dialog.

Requiring SSL for the virtual web sites

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **Device Client**.
- 3 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.
- 4 Expand **Local machine > Default Web Site** and select **WebAPI**.
- 5 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.

Verifying the SSL binding

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 3 Click on **Browse *:443 (HTTPS)** under **Manage Application/Browse Application** (located at the top right corner of the IIS dialog).

You will see this message: *There is a problem with this web site's security certificate.*

Note This message is expected and safe to ignore.

- 4 Click the **Continue to this website (not recommended)** option.
- 5 Verify that the **IIS 7** dialog opens.

Enabling directory browsing in IIS

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **DeviceClient**.

- 3 Double-click on **Directory browsing**.
- 4 In the right **Actions** field, select **ENABLE**.
- 5 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 6 Double-click on **Directory browsing**.
- 7 In the right **Actions** field, select **ENABLE**.

Verifying HTTPS browsing

- 1 Open the IIS Manager.
- 2 Expand the **Default Web Site**.
- 3 Expand **OWS**.
- 4 Select the **Configuration** folder.
- 5 In the actions pane, select **Browse*:443(https)**.
- 6 Select **Continue to this website (not recommended)**.
- 7 Verify that the local page is displayed:
`.../DeviceClient/Configuration/`
- 8 In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
- 9 In the actions pane, select **Browse*:443(https)**.
- 10 Select **Continue to this website (not recommended)**.
- 11 Verify that the localhost page is displayed:
`.../WebAPI/`
- 12 Select **Continue to this website (not recommended)**.

Editing the OmISAPIU.xml file

- 1 Navigate to the following path.
`C:\Program Files (x86)\Omtool\Omtool Server\WebAPI\WebAPI\Scripts`
- 2 In `OmISAPIU.xml`, find the FileTransfer node. Replace the IP address with the OPS Servername or IP. Also, change `http` to `https`.

```
<FileTransfer>https://OPS Servername or IP/WebAPI/FileTransfer/  
</FileTransfer>
```

This OPS Servername is based on the value from Step 10 of [Installing the OPS kit on the server](#).

Note XML files can be edited using Microsoft Notepad.

- 3 Save the file.

Editing the Bootstrap.xml file

- 1 Navigate to the following path:

`C:\Program Files (x86)\Omtool\DeviceClient\Configuration`

- 2 In bootstrap.xml, change `http` to `https`.

```
<Server>https://OPS Servername or IP/webapi/scripts/omisapiu.dll </
Server>
```

This OPS Servername is based on the value from Step 10 of [Installing the OPS kit on the server](#).

- 3 Save the file and reset IIS.

Section 6: Configuring Mixed Devices in the Same Environment (HP Pro, FutureSmart, and OZ)

This section describes the installation and configuration process for a mixed environment of HP Pro, FutureSmart and OZ devices with HTTPS support. This scenario uses the OPS-created certificate for HTTPS communication between all three types of devices and the server.

[Installing the OPS kit on the server](#) (6-1)

[Exporting the OPS server certificate from the Trusted Root Certificate Authorities store for HP Pro devices](#) (6-6)

[Exporting the certificate to the Embedded Device Client directory for FutureSmart and OZ devices](#) (6-7)

[Importing the OPS certificate into the device EWS](#) (6-7)

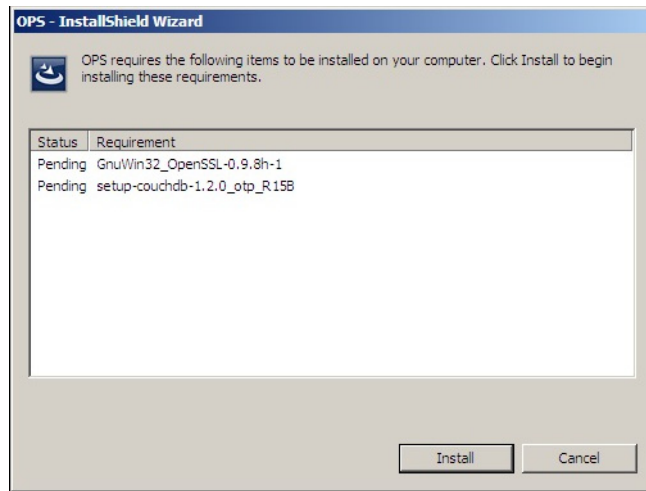
[OPS registration](#) (6-7)

[HTTPS support for HP Pro devices](#) (6-8)

Installing the OPS kit on the server

- 1 On the server, navigate to `C:\Program Files (x86)\Omtool\Omtool Server\Tools`.
- 2 Right-click and select **Run as Administrator**.
- 3 Run `setup.exe` for OPS.
- 4 The OPS InstallShield wizard appears and requests that you install the following two items:
 - ▶ `GnuWin32_OpenSSL-0.9.8h-1`
 - ▶ `setup-couchdb-1.2.0_otp_R15B`

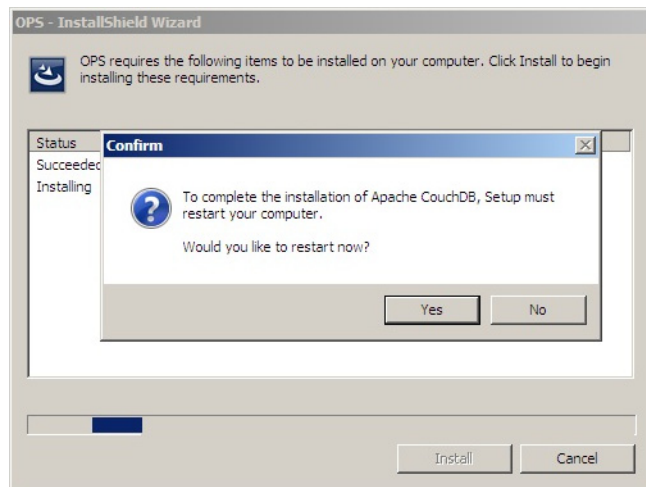
Section 6: Configuring Mixed Devices in the Same Environment (HP Pro, FutureSmart, and OZ)



5 Click **Install**.

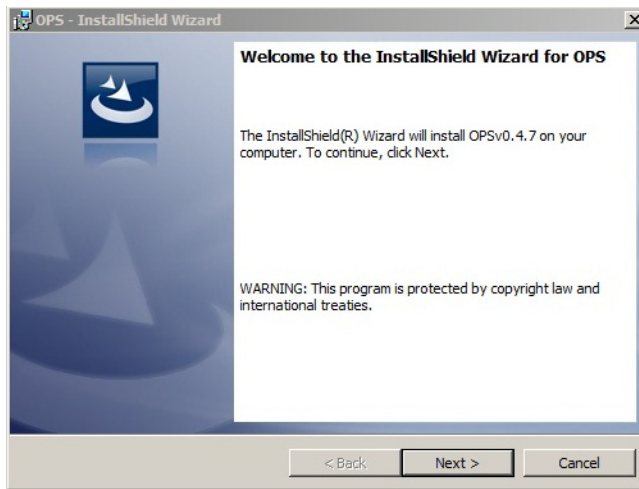
6 After installing the items in Step 3, the following message may appear:

To complete the installation of Apache CouchDB, setup must restart your computer. Would you like to restart now?



If this message appears, click **Yes** to restart. The OPS InstallShield wizard reappears upon restarting the system.

Otherwise, the OPS InstallShield wizard **Welcome** screen immediately appears.

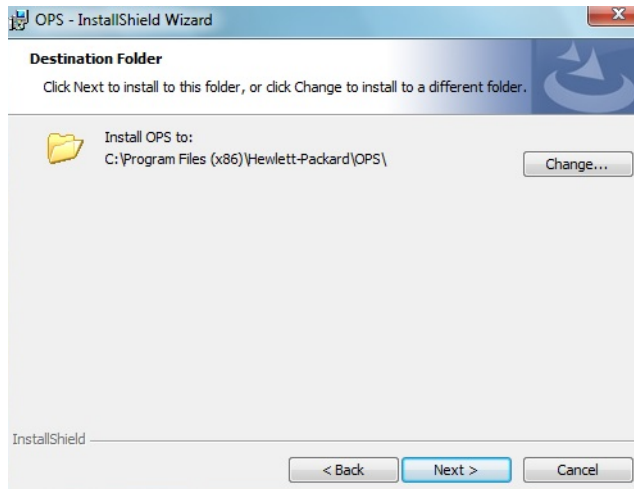


7 Click **Next**. The **License Agreement** screen appears.

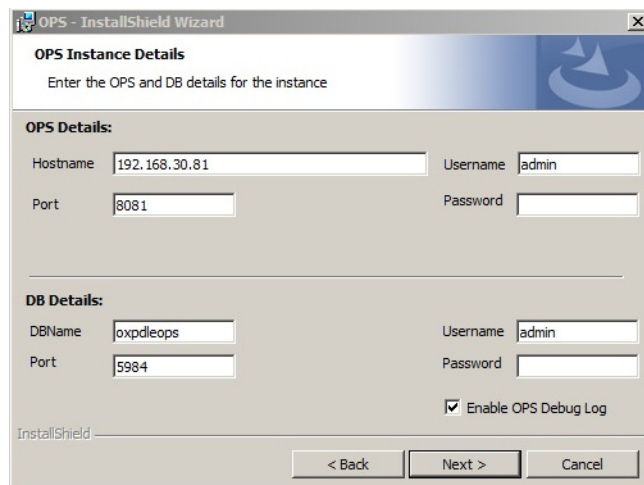


8 Select **I accept the terms in the license agreement** and click **Next**.

The **Destination Folder** screen appears.

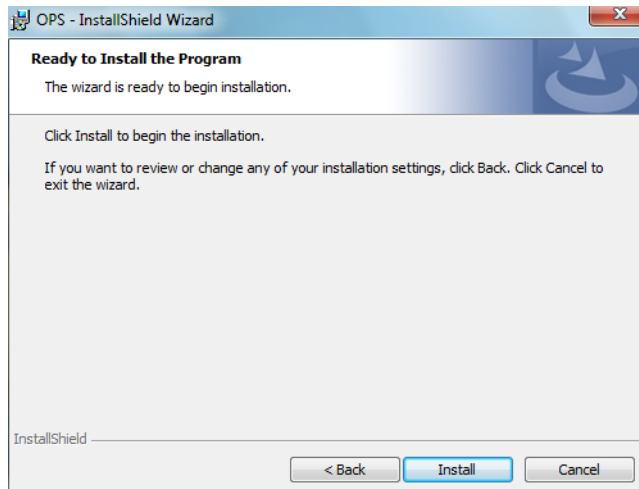


9 Click **Next**. The **OPS Instance Details** screen appears.



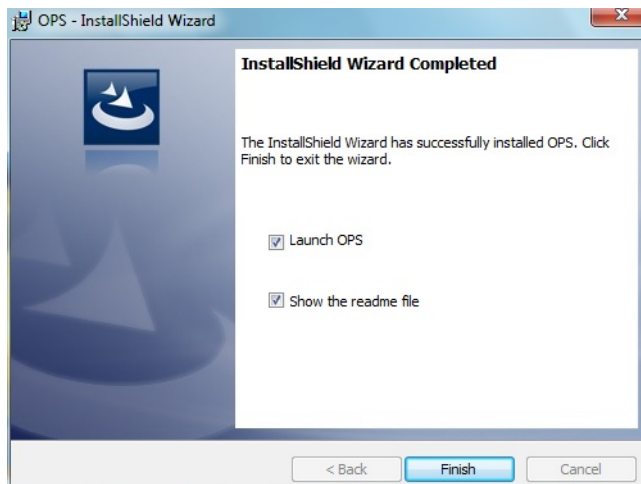
- 10** In the **Hostname** field enter either the IP or FQDN of the server on which OPS is installed. This value is the OPS server name. Make note of this value, as you will need to reference it later during device registration and HTTPS configuration.
- 11** Enter the **Passwords** in both the **OPS Details** and **DB Details** sections. Also make note of these for later use.

12 Click Next.The **Ready to Install the Program** screen appears.



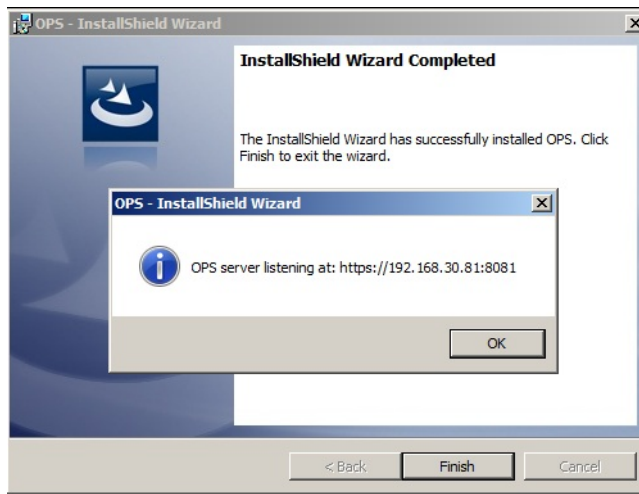
13 Click Install.

14 The OPS InstallShield Wizard Completed screen appears.

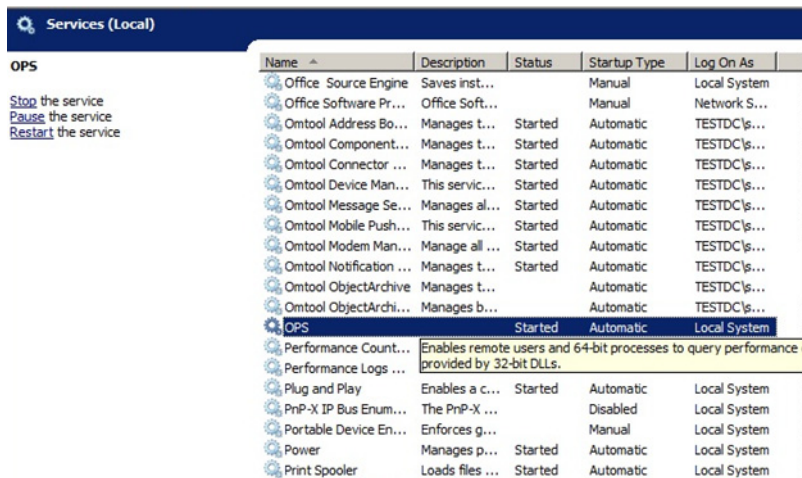


Select both the **Launch OPS** and **Show the readme file** check boxes (**Show the readme file** is optional) and then click **Finish**.

A pop-up message appears to inform you that the OPS server is listening at the IP address and port listed in step 9.



Click **OK**. OPS now appears as a Windows service.



Exporting the OPS server certificate from the Trusted Root Certificate Authorities store for HP Pro devices

- 1 Open a Windows console and select **File > Add /Remove snap in...**
- 2 Select **Certificates** and click the **Add** button. The **Certificates** snap-in wizard appears.
- 3 Select the **Computer account** radio button and click **Next**, **Finish** and **OK**.
- 4 The console loads with the new Certificate snap-in.
- 5 Expand **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.

- 6 Right-click the **OPS certificate** and select **All tasks > Export**.
- 7 The **Certificate Export** wizard appears. Select **Next**.
- 8 Choose **Base-64 encoded x.509(.CER)** and select **Next**.
- 9 Name the file and select **Browse**.
- 10 Place the certificate in `C:\Program Files (x86)\Hewlett-Packard\OPS`.
- 11 Select **Next** and then click **Finish**.

Exporting the certificate to the Embedded Device Client directory for FutureSmart and OZ devices

- 1 Navigate to `C:\Program Files (x86)\Hewlett-Packard\OPS` and copy the certificate saved from previous steps.
- 2 Navigate to and then paste the certificate into `C:\Program Files (x86)\Omtool\DeviceClient\Certificate\OPS`.

All FutureSmart and Oz devices will use this Certificate for HTTPS communication.

Importing the OPS certificate into the device EWS

- 1 Open and log into the EWS of the Pro Device.
- 2 On the **Network** tab select **Advanced settings > Certificates**.
- 3 Select **Import > Choose File**.
- 4 Browse to the location where the OPS certificate was saved and select **Open** and then **Finish**.

OPS registration

- 1 At a command prompt enter
`C:\Program Files (x86)\Hewlett-Packard\OPS\bin>OPSSetup`
- 2 You will be prompted to choose from a selection of options.
Select **Option 3: Register a device to the OPS server**.
- 3 Enter the IP address for the device. For example, `123.456.78.9`.
- 4 Enter the device **username** and **password** you want to use, noted from [Installing the OPS kit on the server](#) (6-1).

- 5 Enter the **OPS server URL** you want to register. For example, `https://<hostname or IP>:port`.
- 6 Enter the **username** and **password** for the OPS server.

Note The OPS server URL and username can be obtained from Steps 8 and 9 above in [Installing the OPS kit on the server \(6-1\)](#).

- 7 The following message appears:

```
OPS Registered successfully
```

Your local OPS server is now installed. See [Creating a group of devices \(part I\) \(6-41\)](#) for more information on creating device groups.

HTTPS support for HP Pro devices

Note When using a remote OPS server, to use the OPS-created certificate for an HTTPS environment, make sure the OPS server is installed on the remote system.

Creating an SSL binding

- 1 Open the IIS Manager.
- 2 Click on the **Default Web Site** and locate **Bindings** under **Edit Site** (top right corner of the window).
- 3 Click on **Bindings**. The **Site Bindings** dialog opens.
- 4 Click on **HTTPS type** and select **Edit**. The **Edit Site Bindings** dialog opens.
- 5 In the **SSL certificate** drop-down, choose the certificate that was created earlier and click **OK**.
- 6 Click **Close** to close the dialog.

Requiring SSL for the virtual web sites

- 7 Open the IIS Manager.
- 8 Expand **Local Machine > Default Web Site** and select **Device Client**.
- 9 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.
- 10 Expand **Local machine > Default Web Site** and select **WebAPI**.
- 11 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.

Verifying the SSL binding

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 3 Click on **Browse *:443 (HTTPS)** under **Manage Application/Browse Application** (located at the top right corner of the IIS dialog). You will see this message:

There is a problem with this web site's security certificate.

Note This message is expected and safe to ignore.

- 4 Click the **Continue to this website (not recommended)** option.
- 5 Verify that the **IIS 7** dialog opens.

Enabling directory browsing in IIS

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **DeviceClient**.
- 3 Double-click on **Directory browsing**.
- 4 In the right **Actions** field, select **ENABLE**.
- 5 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 6 Double-click on **Directory browsing**.
- 7 In the right **Actions** field, select **ENABLE**.

Verifying HTTPS browsing

- 1 Open the IIS Manager.
- 2 Expand the **Default Web Site**.
- 3 Expand **OWS**.
- 4 Select the **Configuration** folder.
- 5 In the actions pane, select **Browse*:443(https)**.
- 6 Select **Continue to this website (not recommended)**.
- 7 Verify that the local page is displayed. For Embedded Device Client:

```
.../DeviceClient/Configuration/
```
- 8 In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
- 9 In the actions pane, select **Browse*:443(https)**.
- 10 Select **Continue to this website (not recommended)**.
- 11 Verify that the localhost page is displayed:

```
.../WebAPI/
```

- 12 Select **Continue to this website (not recommended)**.

Editing the OmISAPIU.xml file

- 1 Navigate to the following path.

```
C:\Program Files (x86)\Omtool\Omtool Server\WebAPI\WebAPI\Scripts
```

- 2 In `OmISAPIU.xml`, find the `FileTransfer` node. Replace the IP address with the fully qualified domain name. Also, change `http` to `https`.

```
<FileTransfer>https://OPS Servername or IP/WebAPI/FileTransfer/  
</FileTransfer>
```

This OPS Servername is based on the value from Step 10 of [Installing the OPS kit on the server](#).

Note XML files can be edited using Microsoft Notepad.

- 3 Save the file.

Editing the Bootstrap.xml file

- 1 Navigate to the following path:

```
C:\Program Files (x86)\Omtool\DeviceClient\Configuration
```

- 2 In `bootstrap.xml`, change `http` to `https`.

```
<Server>https://OPS Servername or IP/webapi/scripts/omisapiu.dll </  
Server>
```

This OPS Servername is based on the value from Step 10 of [Installing the OPS kit on the server](#).

- 3 Save the file.
- 4 Reset IIS.

Section 6: Configuring Mixed Devices in the Same Environment (HP Pro, FutureSmart, and OZ)

Section 7: Required Configuration

This section describes:

[Adding devices using the AccuRoute Server Administrator](#) (7-1)

[Choosing an authentication method](#) (7-26)

[Configuring the server](#) (7-29)

See also [Section 10: Testing](#) (10-77) and the [AccuRoute server administrator on-line help](#) (for additional information including optional configurations, testing, and troubleshooting).

Adding devices using the AccuRoute Server Administrator

This section describes the procedures for:

[Creating a group of devices \(part 1\)](#) (7-1)

[Creating a group of devices \(part 2\)](#) (7-6)

[Updating the DeviceLoader.xml to support new devices](#) (7-23)

[Adding a new device](#) (7-23)

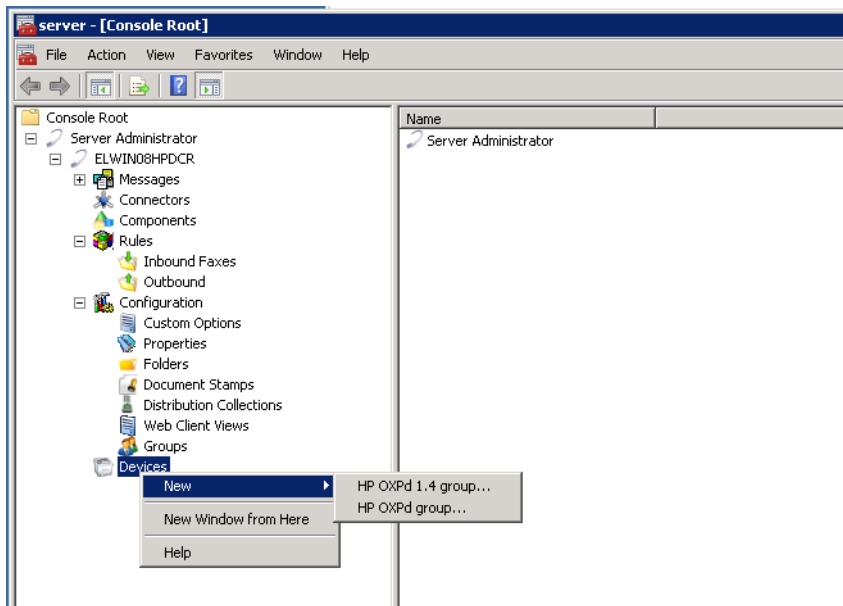
Creating a group of devices (part 1)

Create a new Group for each group of devices. While each group may have the same configuration, you can configure a group to have a configuration that is completely different from another group. For example, you might create a group named “Marketing” and configure it to use only the Routing Sheets and Fax features. You might create an additional group named “Sales” and configure it for PIN authentication and ability to use only the Routing Sheet, Personal Distributions, and Scan to Me features.

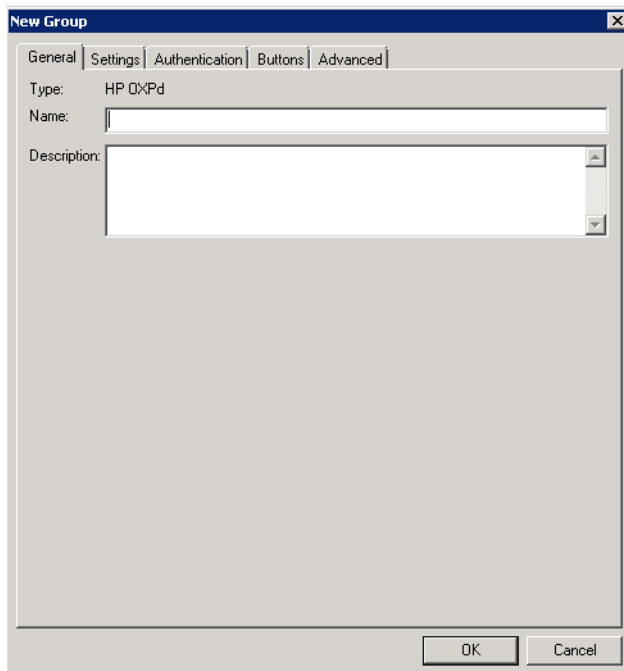
The following procedure explains how to create and configure a group.

- 1 Click **Start > All Programs > Omtool > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute server.
- 3 Go to the **Devices** node.
- 4 Right-click and select **New > Embedded Device group**.

Section 7: Required Configuration

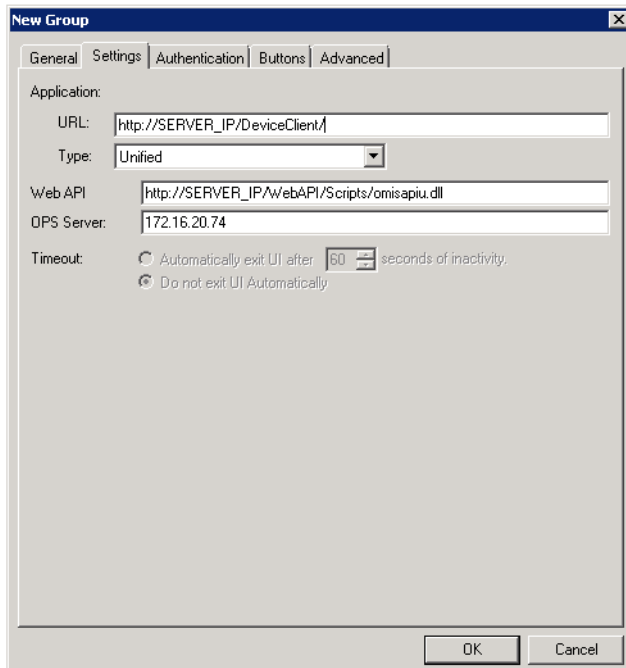


The **New Group** page opens.



- 5 In the **Name** text box, enter a name for the device.
- 6 Optionally, in the **Description** text box, enter a device description.

- 7 Click the **Settings** tab. Change settings *only* if the IIS/Web server is remote or if you are configuring HTTPS.



- If you are configuring for HTTPS, change the URL path from HTTP to HTTPS. For example:
Application URL: <https://FQDN/DeviceClient/>
Web API: <https://FQDN/WebAPI/Scripts/omisapiu.dll>
- If you are configuring a device group of HP Pro devices, confirm the IP address of the OPS Server in the **OPS Server** field.
- For remote systems – If you installed the AccuRoute Embedded Device Client on a remote system, you must manually enter the IP address of that system in the URL field.
- If you are using a local OPS server and an OPS-created certificate for HTTPS environments, change the Application and WebAPI's URLs to <https://IP address> or FQDN name to match the OPS server. Then continue on to the following sub-sections [Creating an SSL binding](#) (7-3) through to [Editing the OmlSAPIU.xml file](#) (7-5).

Otherwise, continue these steps below at [Creating a group of devices \(part 2\)](#) (7-6).

Important The following sub-sections are for users with a local OPS server and an OPS-created certificate for HTTPS environments.

Creating an SSL binding

- 1 Open the IIS Manager.
- 2 Click on the **Default Web Site** and locate **Bindings** under **Edit Site** (top right corner of the window).
- 3 Click on **Bindings**. The **Site Bindings** dialog opens.

- 4 Click on **HTTPS type** and select **Edit**. The **Edit Site Bindings** dialog opens.
- 5 In the **SSL certificate** drop-down, choose the certificate that was created earlier and click **OK**.
- 6 Click **Close** to close the dialog.

Requiring SSL for the virtual web sites

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **OXF DeviceClient**.
- 3 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.
- 4 Expand **Local machine > Default Web Site** and select **WebAPI**.
- 5 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.

Verifying the SSL binding

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 3 Click on **Browse *:443 (HTTPS)** under **Manage Application/Browse Application** (located at the top right corner of the IIS dialog). You will see this message:

There is a problem with this web site's security certificate.

Note This message is expected and safe to ignore.

- 4 Click the **Continue to this website (not recommended)** option.
- 5 Verify that the **IIS 7** dialog opens.

Enabling directory browsing in IIS

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **Embedded Device Client**.
- 3 Double-click on **Directory browsing**.
- 4 In the right **Actions** field, select **ENABLE**.
- 5 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 6 Double-click on **Directory browsing**.
- 7 In the right **Actions** field, select **ENABLE**.

Verifying HTTPS browsing

- 1 Open the IIS Manager.
- 2 Expand the **Default Web Site**.
- 3 Expand **Embedded Device Client**.
- 4 Select the **Configuration** folder.
- 5 In the actions pane, select **Browse*:443(https)**.

- 6 Select **Continue to this website (not recommended)**.
- 7 Verify that the local page is displayed.
For the AccuRoute Embedded Device Client:
`.../DeviceClient/Configuration/`
- 8 In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
- 9 In the actions pane, select **Browse*:443(https)**.
- 10 Select **Continue to this website (not recommended)**.
- 11 Verify that the **localhost** page is displayed:
`.../WebAPI/`
- 12 Select **Continue to this website (not recommended)**.

Editing the OmISAPIU.xml file

- 1 Navigate to the following path.
`C:\Program Files (x86)\Omtool\Omtool Server\WebAPI\WebAPI\Scripts`
- 2 In `OmISAPIU.xml`, find the **FileTransfer** node. Replace the IP address with the fully qualified domain name. Also, change `http` to `https`.

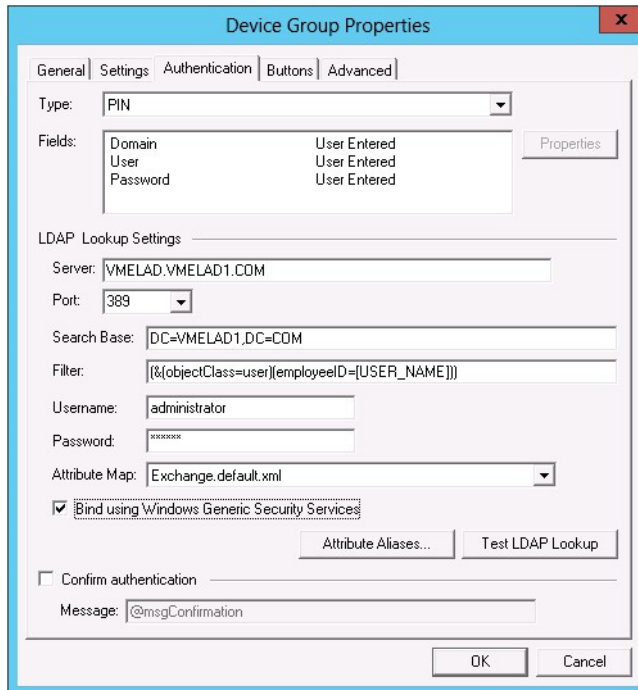
```
<FileTransfer>https://fully_qualified_domain_name/WebAPI/  
FileTransfer/  
</FileTransfer>
```

Note XML files can be edited using Microsoft Notepad.

- 3 Save the file and continue with [Creating a group of devices \(part 2\)](#) below.

Creating a group of devices (part 2)

- 1 Click the **Authentication** tab to specify the type of user authentication required for the group of devices.



The screenshot shows the 'Device Group Properties' dialog box with the 'Authentication' tab selected. The 'Type' dropdown is set to 'PIN'. The 'Fields' section shows 'Domain', 'User', and 'Password' all set to 'User Entered'. The 'LDAP Lookup Settings' section includes: Server: VMELAD.VMELAD1.COM, Port: 389, Search Base: DC=VMELAD1,DC=COM, Filter: (&(objectClass=user)(employeeID=[USER_NAME])), Username: administrator, Password: [masked], Attribute Map: Exchange.default.xml. There is a checked checkbox for 'Bind using Windows Generic Security Services' and buttons for 'Attribute Aliases...' and 'Test LDAP Lookup'. At the bottom, there is an unchecked checkbox for 'Confirm authentication' and a 'Message:' field containing '@msgConfirmation'. 'OK' and 'Cancel' buttons are at the bottom right.

- 2 From the **Type** drop-down, select one of the three authentication options: **Email**, **Login**, or **PIN**.
After you select **Email**, **Login**, or **PIN** as the authentication type, you can define the properties for the **Domain**, **User**, and **Password** in the **Fields** section.
Domain, **User**, and **Password** properties are described on the following pages.

Defining Domain Properties

To define domain properties, double-click **Domain**. The **Domain Field Properties** dialog is displayed:

The screenshot shows the 'Domain Field Properties' dialog box. It has a title bar with a close button. The dialog contains the following elements:

- Label:** A text box containing '@authDomainLabel'.
- Default value:** An empty text box.
- User must enter a value for Domain** (selected radio button):
 - Enable input validation
 - Regular Expression:** An empty text box.
 - Error message:** A text box containing '@authDomainErrorText'.
- User must select a value for Domain from one of the following:** (selected radio button):
 - A list box (currently empty).
 - Buttons: Add..., Remove, Set Default, ^, v.
- User may not enter a value for Domain** (selected radio button):
 - Display the default value to the user (read-only)
- OK** and **Cancel** buttons at the bottom.

When you define a domain, you can specify a **Default value** (domain) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for Domain** - The device user will need to enter a domain for authentication during login at the device.
- **User must select a value for Domain from one of the following** - If there are multiple domains in the environment, use this option to create a list of domains from which the user can select.
- **User may not enter a value for Domain** - This option prohibits the user from entering a domain value. When you select this option, you can indicate that the device will **Display the default value to the user (read-only)**. The user will see the **Default value**, but cannot change it.

Note Domain definition is optional for all authentication types.

Defining User Properties

To define user properties, double-click **User**. The **User Field Properties** dialog is displayed:

When you define a user, you can specify a **Default value** (user) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for User** - The device user will need to enter a user for authentication during login at the device.
- **User must select a value for User from one of the following** - If there are multiple users in the environment, use this option to create a list from which the user can select.
- **User may not enter a value for User** - Do not select this option if you are using Email, Login, or PIN authentication. This option prohibits the user from entering a user value.

When you select this option, you can indicate that the device will **Display the default value to the user (read-only)**. The user will see the **Default value**, but cannot change it.

Note User definition is required for **Login** authentication and optional for all other authentication types.

Defining Password Properties

To define user properties, double-click **User**. The **User Field Properties** dialog is displayed:

The screenshot shows the "Password Field Properties" dialog box. It has a title bar with a close button. The "Label:" field contains "PW". The "Default value:" field is empty. The "User must enter a value for Password" radio button is selected. Under this option, "Enable input validation" is unchecked. The "Regular Expression:" field is empty, and the "Error message:" field contains "@authPasswordErrorText". The "User must select a value for Password from one of the following:" radio button is unselected. Below it is an empty list box and buttons for "Add...", "Remove", "Set Default", and up/down arrows. The "User may not enter a value for Password" radio button is unselected. Below it, "Display the default value to the user (read-only)" is unchecked. At the bottom are "OK" and "Cancel" buttons.

When you define a password, you can specify a **Default value** (password) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for Password** - The device user will need to enter a password for authentication during login at the device.
- **User must select a value for Password from one of the following** - If there are multiple passwords available in the environment, use this option to create a list from which the user can select.
- **User may not enter a value for Password** - This option prohibits the user from entering a password. Use this option only when PIN authentication is used without a password. Do not select this option if you are using Email, Login, or PIN (with password) authentication.

When you select this option, you can indicate that the device will **Display the default value to the user (read-only)**. The user will see the **Default value**, but cannot change it.

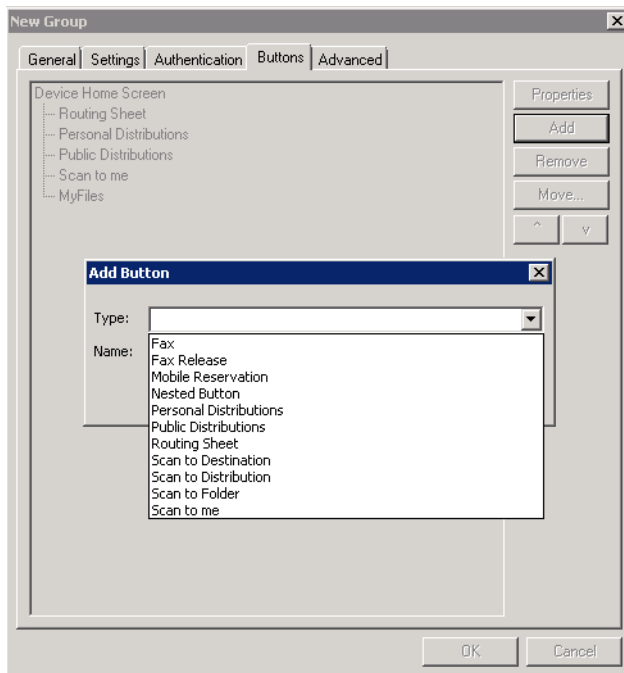
Note Password definition is required for **Login** authentication and optional for all other authentication types.

- 3 After you define **Domain**, **User**, and/or **Password** properties, click **OK** to return to the **Device Group Properties** page. For example

The screenshot shows the 'New Group' dialog box with the 'Authentication' tab selected. The 'Type' is set to 'Email'. The 'Fields' section shows 'Domain', 'User', and 'Password' all set to 'User Entered'. The 'LDAP Lookup Settings' section includes: Server: VMELAD.VMELAD1.COM, Port: 389, Search Base: DC=VMELAD1,DC=COM, Filter: (&{objectClass=user}([proxyAddresses=SMTP:[USER_NAME]])), Username and Password text boxes, Attribute Map: Exchange.default.xml, and a checked checkbox for 'Bind using Windows Generic Security Services'. There are buttons for 'Attribute Aliases...', 'Test LDAP Lookup', 'Confirm authentication', 'Message: @msgConfirmation', 'OK', and 'Cancel'.

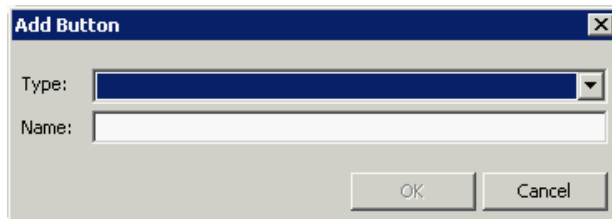
- 4 In the **Username** text box, enter the name of a Windows user who has permissions to query the active directory.
- 5 In the **Password** text box, enter the Administrator password.
- 6 Select the **Confirm authentication** option if you want to display a prompt on the device to verify the user's information when authenticating.

- 7 Click the **Buttons** tab where you can add or remove buttons that appear on the device.



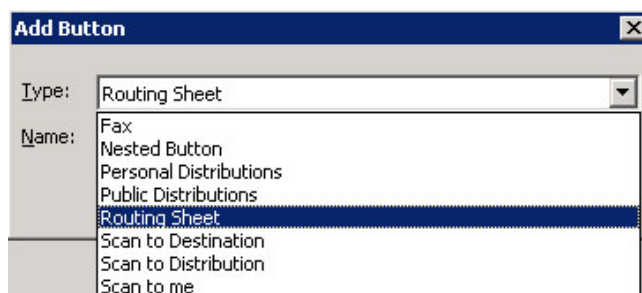
Note It is best to add or remove buttons before installing to the device. Otherwise, if buttons are added or removed, or if button text is modified, it will be necessary to uninstall and run the installation again.

- 8 To add a button, click **Add**. The **Add Button** dialog is displayed.



Note If the **Add** button is not active, click on **Device Home Screen**.

- 9 From the **Type** drop-down, select a button type.



10 Enter a **Name** for the button. Then, click **OK**.

11 You will need to define properties for the button. With the button highlighted on the list, click **Properties**.

Each button has a default **Name**, **Display Text**, and **Description** that you can edit.

Note Do not change **Image** from the default value.

Note For buttons requiring authentication, select **Capture user password** for the credential pass-through feature and **Always prompt user for password** for use with HPAC authentication.

12 Specify a location for the button. Select either of these options:

- **Auto assign based on configured ordering** - The button is positioned based on a predefined order.
- **Use specific ordering priority** - You can enter a value to indicate the button placement. Position 1 is in the upper left location and position 2 is in the upper right location, in a Z-order layout. The pattern is as follows:

```

1 2
3 4
5 6
etc.

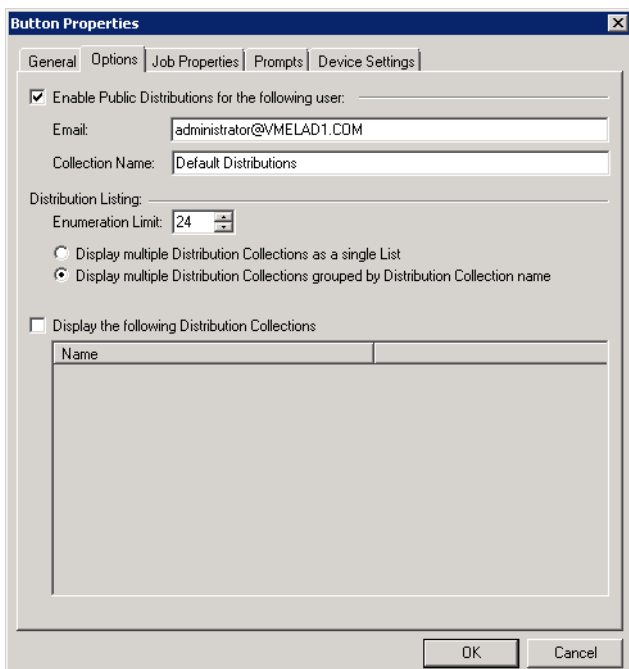
```

13 Select addition options for the button:

- ▶ **Enable this button for use on the device** - Self-explanatory.
- ▶ **Enable job build** - This option enables the Scan More feature.

- ▶ **Enable One-Touch scanning** - This allows the user to select a button with the documents already loaded in the Automatic Document Feeder for one-touch scanning. Typically, this is used with a Distribution that has all scan settings saved.
- ▶ **Enable scan preview by default (only on supported devices)** - This applies to **FutureSmart** devices only.
- ▶ **Require authentication** - If you select this option, you can then indicate that the button should capture the user's password. Note that although the Routing Sheet feature typically does not require authentication, you can configure this requirement here.

I4 If you are adding a **Personal Distributions** or **Public Distributions** button, click the **Options** tab.

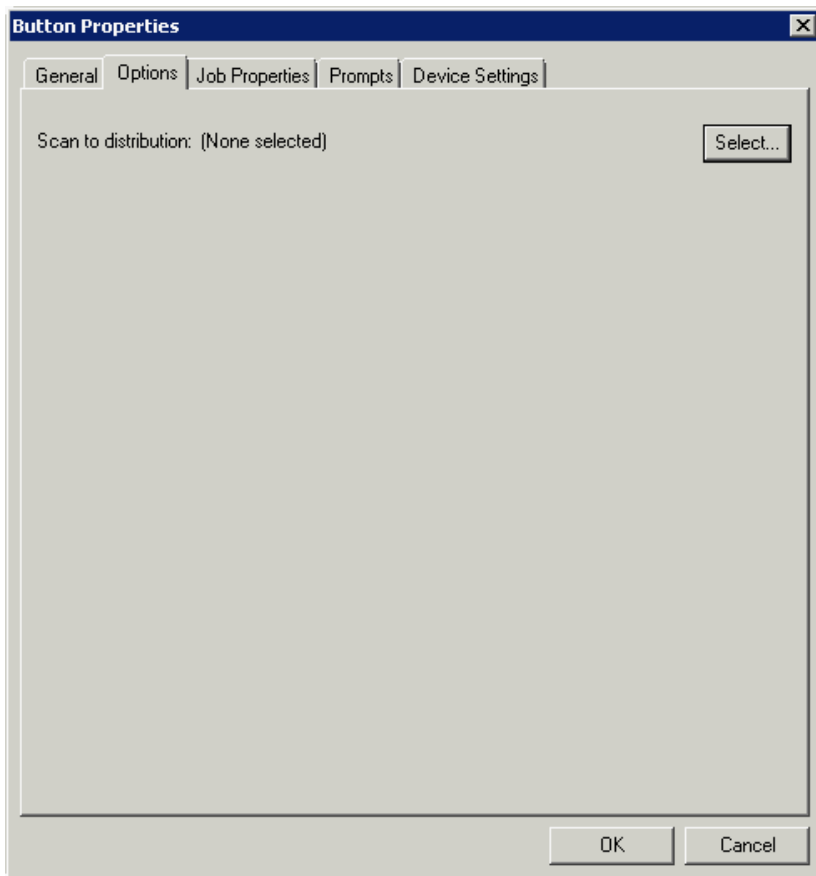


The screenshot shows the 'Button Properties' dialog box with the 'Options' tab selected. The 'Enable Public Distributions for the following user:' checkbox is checked. The 'Email' field contains 'administrator@VMELAD1.COM' and the 'Collection Name' field contains 'Default Distributions'. Under 'Distribution Listing', the 'Enumeration Limit' is set to 24. The radio button for 'Display multiple Distribution Collections grouped by Distribution Collection name' is selected. The 'Display the following Distribution Collections' checkbox is unchecked, and the table below it is empty.

Name

Enter a **Public Email** address (if applicable) and set the **Enumeration Limit** for distributions (the maximum number of distributions allowable).

- 15 If you are adding a **Scan to Distribution** button, click the **Options** tab to route using an existing (already created) distribution.



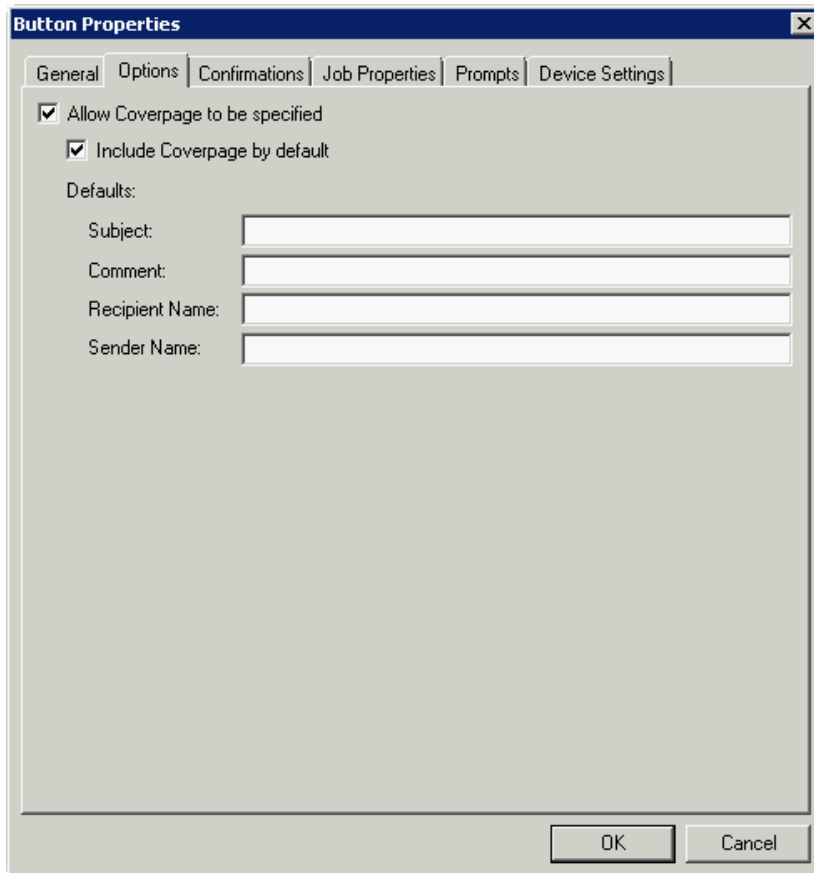
Click **Select** and the **Select Embedded Directive** dialog is displayed.

Title ▲	Owner	Created	Last Used	Single Use	Expires
---------	-------	---------	-----------	------------	---------

Click the **Find** button to display all distributions.

Select the distribution and then click the **Select** button to choose the distribution that will be used when that button is selected from the device.

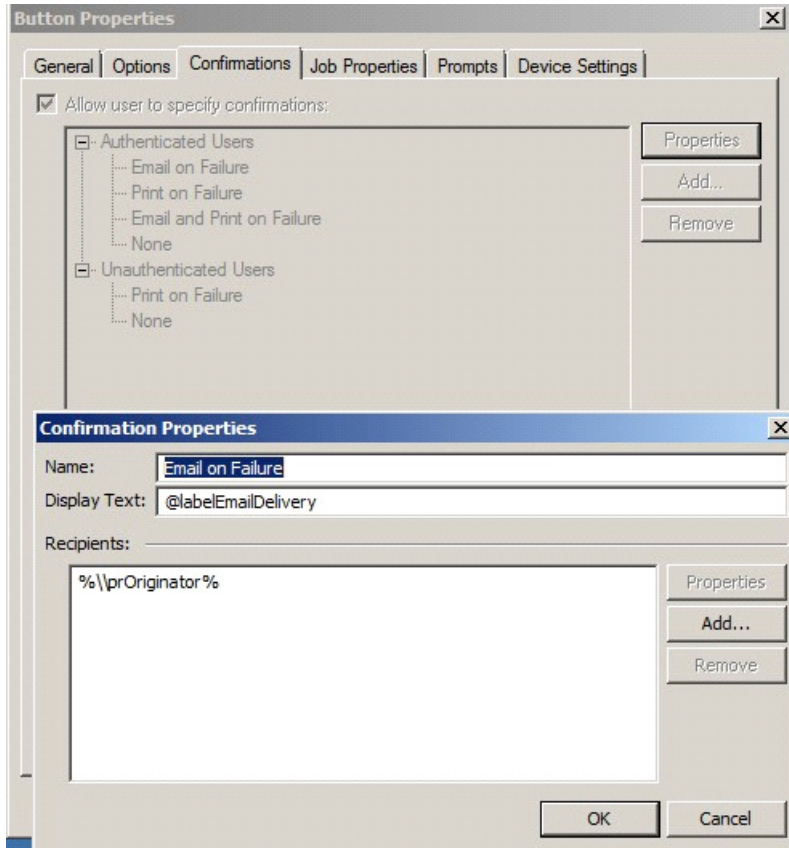
- 16** If you are adding a **Fax** button, click the **Options** tab to configure fax cover pages. Select options to allow a cover page to be specified and include the cover page by default. In addition, you can indicate the information (subject, etc.) that will appear on the cover page.



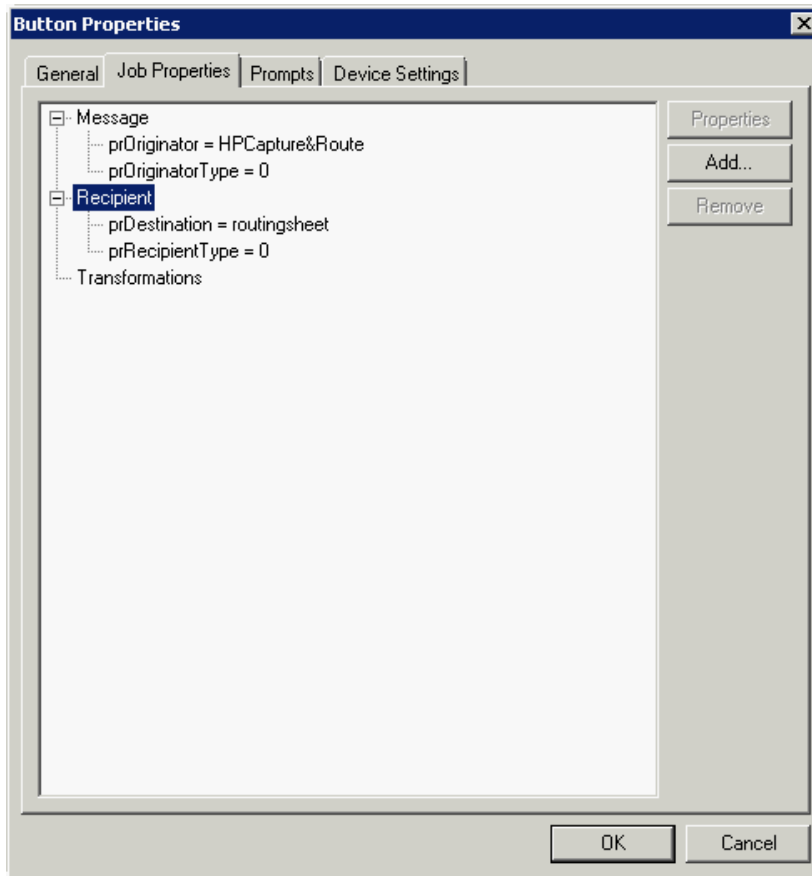
The image shows a screenshot of the "Button Properties" dialog box, specifically the "Options" tab. The dialog box has a title bar with a close button (X) and a tabbed interface with the following tabs: "General", "Options", "Confirmations", "Job Properties", "Prompts", and "Device Settings". The "Options" tab is selected. Inside the dialog, there are two checked checkboxes: "Allow Coverpage to be specified" and "Include Coverpage by default". Below these checkboxes, there is a section labeled "Defaults:" with four text input fields: "Subject:", "Comment:", "Recipient Name:", and "Sender Name:". At the bottom right of the dialog, there are "OK" and "Cancel" buttons.

- 17** If you are adding a **Fax** button, click the **Confirmations** tab to:
- ▶ Allow authenticated and non-authenticated users to select the button.
 - ▶ Define the type of fax confirmations (select a field and click **Properties**).
 - ▶ Add recipients for confirmations (click the **Add** button).

For example, you can edit the fields for the Originator for faxed faxes:



- 18 If you are adding a **Routing Sheet**, **Scan to Destination**, **Scan to Distribution**, **Scan to Me**, or **Scan to My Files** button, click the **Job Properties** tab.



You can add, remove, or change a property. This example shows the property of a **Destination**.

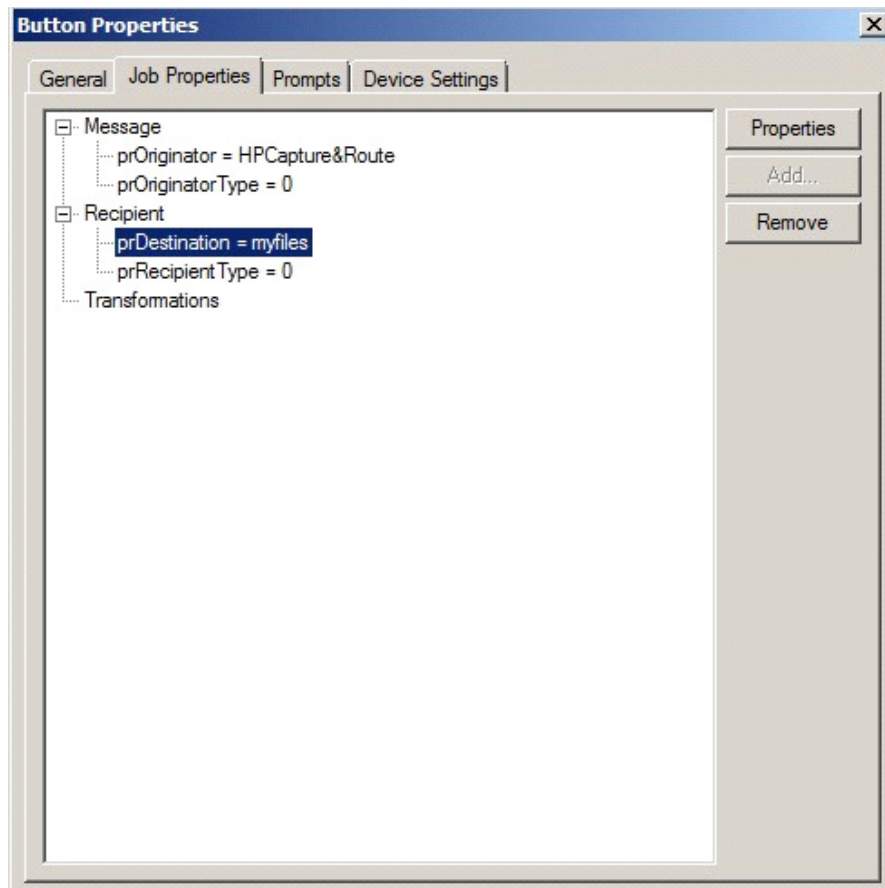


You can change an **Originator**, **Destination**, or **Recipient**. You also can add a **Transformation** (replacing a data value (a message property, recipient property, Embedded Directive property, or template variable) with another value.).

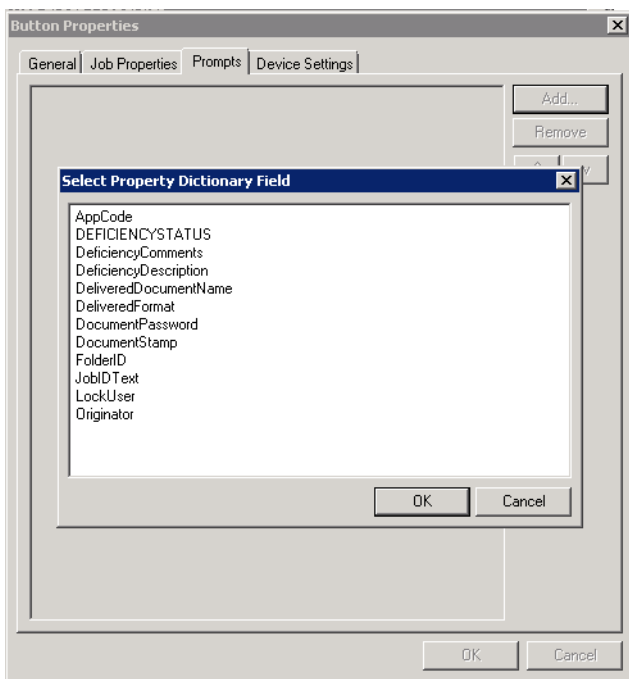
Note that the **Scan to Destination** button allows for message routing based on routing rules.

- ▶ The default is set to send to a destination of MyFiles, which can have an outbound rule associated with that destination to route to any location to which the AccuRoute server can route messages. This destination value can be edited.

- ▶ Transformations can also be added here.

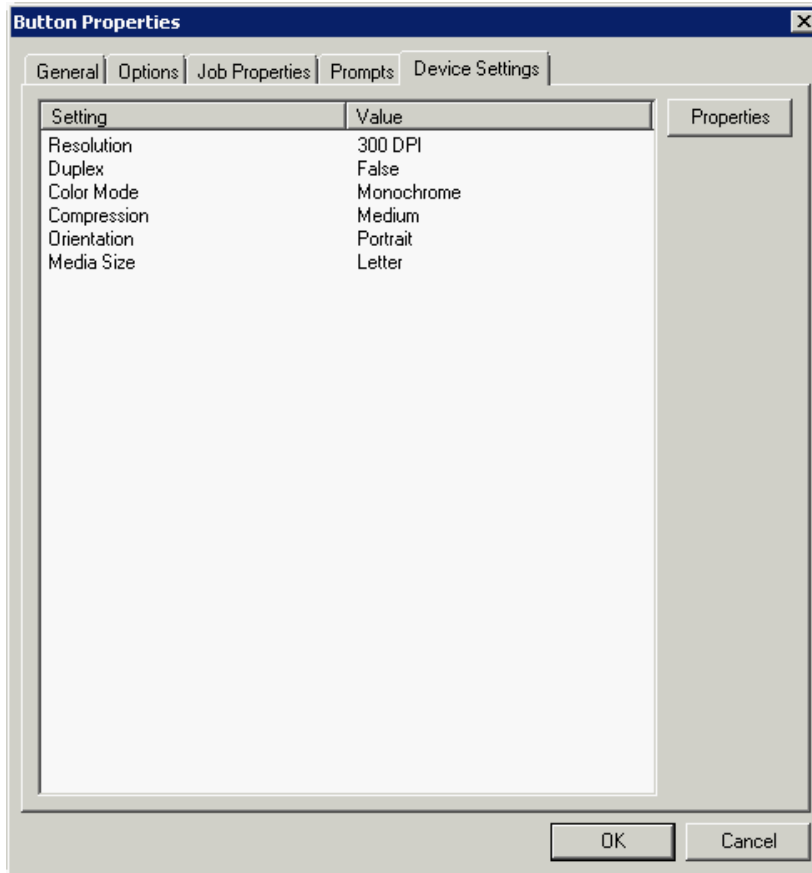


19 Click the **Prompts** tab. Click **Add** to select a prompt configured on the AccuRoute server. The **Select Property Dictionary Field** is displayed.

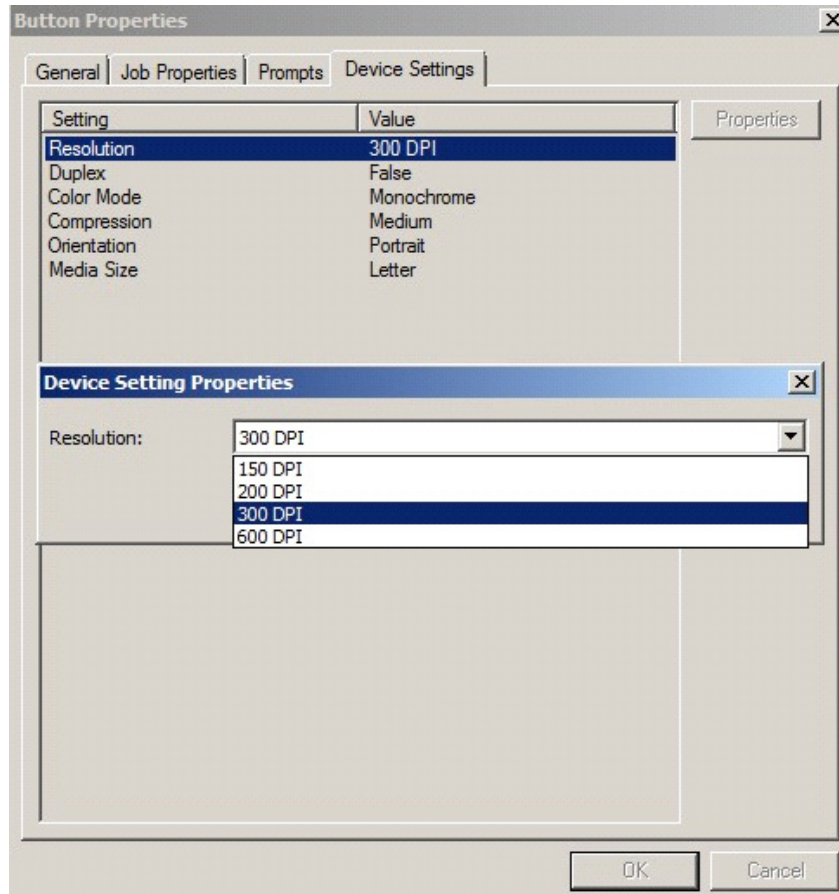


Select a prompt and click **OK**.

- 20** Click the **Device Setting** tab to configure native device scan settings. This is used for configuring a fleet of monochrome or color machines to use the same scanning settings. For example, the Fax button should only use Monochrome scan settings for better output quality.



Select a setting and click **Properties** to change the setting value. For example:



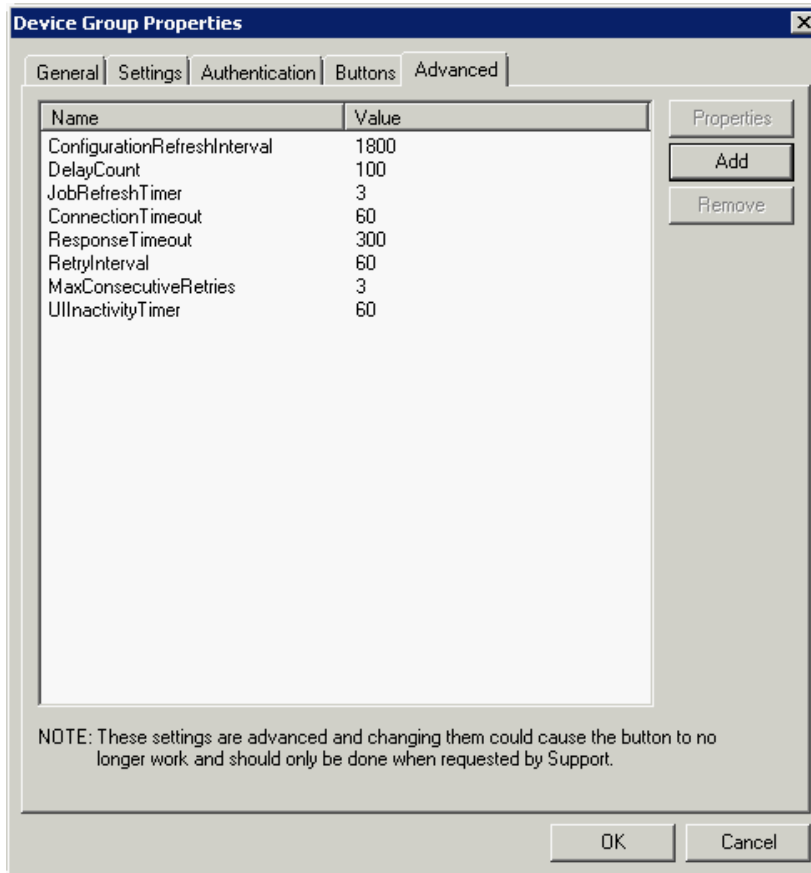
Note The HP Officejet Pro 276dw does not support 600 x 600 scanning with the AccuRoute Embedded Device Client.

21 Click **OK** to return to the **Device Group Properties**.

Note All features/settings within each button can be configured after the button has been installed to a device and are updated instantaneously after selecting **OK**. Uninstallation and re-installation are required only if a button is added or removed, or if the button text is modified.

22 Click the **Advanced** tab to modify settings that control the device's native settings for connectivity timeouts and job refresh settings.

Note Take note of all defaults before changing any of these settings.



23 Click **OK** to end your work with the **Device Group Properties**.

24 Once a button configuration is complete, the xml files can be exported for importing into AccuRoute's WebJet Admin server for button deployment.

Go to the **Devices** node and right-click on the group name. Then, select the **Export to Web Jet Admin** option. See [Installing HP CR Embedded Device Client buttons](#) (9-66).

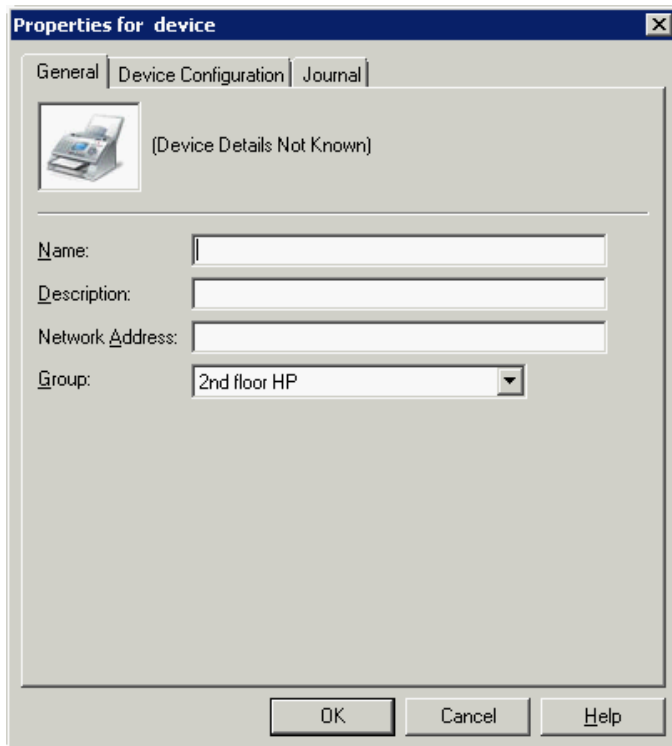
Updating the Deviceloder.xml to support new devices

If you need to update the [Deviceloder.xml](#) to include new devices, refer to the [AccuRoute server administrator on-line help](#).

Adding a new device

- 1 In the console tree, expand the AccuRoute server and go to the **Devices** node.
- 2 Right-click and select the group name. Then, select **New > Device**.

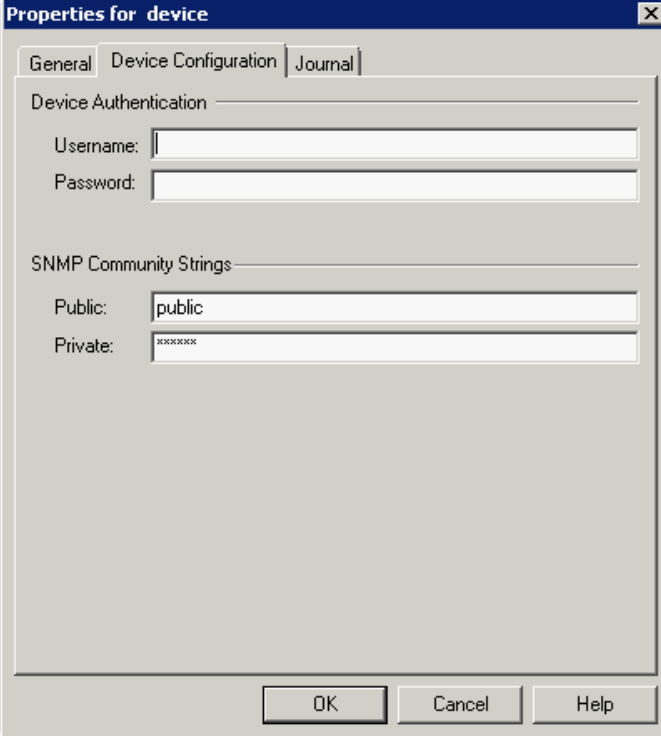
The **Properties for device** page opens.



The screenshot shows a Windows-style dialog box titled "Properties for device". It has three tabs: "General", "Device Configuration", and "Journal". The "General" tab is selected. Inside the dialog, there is a printer icon and the text "(Device Details Not Known)". Below this, there are four input fields: "Name:" (text box), "Description:" (text box), "Network Address:" (text box), and "Group:" (dropdown menu with "2nd floor HP" selected). At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

- 3 In the **Name** text box, enter a name for the device.
- 4 Optionally, in the **Description** text box, enter a device description.
- 5 In the **Network Address** text box, enter the device IP address.

6 Click the **Device Configuration** tab.



The screenshot shows a dialog box titled "Properties for device" with a close button (X) in the top right corner. The dialog has three tabs: "General", "Device Configuration", and "Journal". The "Device Configuration" tab is selected. The dialog is divided into two sections: "Device Authentication" and "SNMP Community Strings".

Device Authentication

Username:

Password:

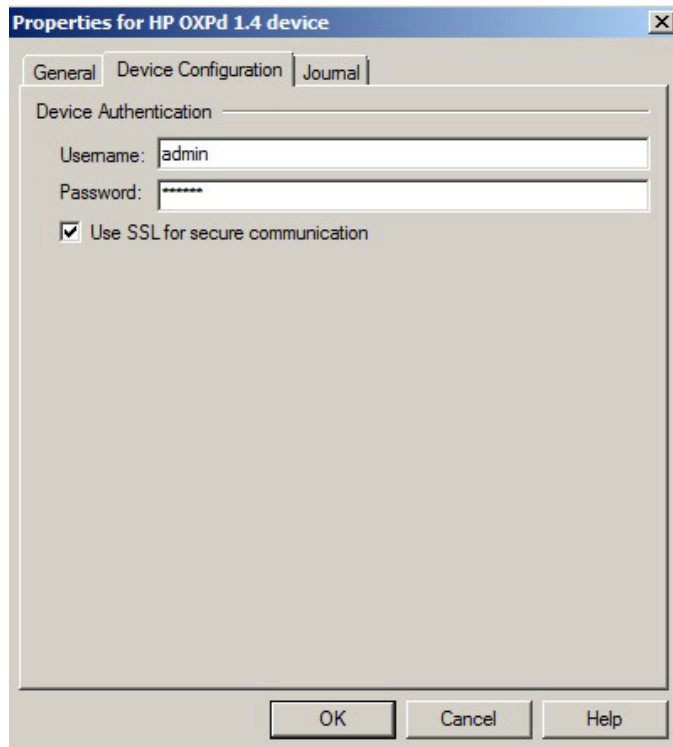
SNMP Community Strings

Public:

Private:

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

When installing to an AccuRoute Embedded Device Client using HTTPS, you must select the **Use SSL for secure communication** option.



- 7 In the **Username** text box, enter the device Administrator name.
- 8 In the **Password** text box, enter the Administrator password.
- 9 If you are using the AccuRoute Embedded Device Client, configure the **SNMP Community Strings** section (this section will not appear for HP OXPd v1.4).
 - ▶ In the **Public** text box, enter the v1.6 device public community string.
 - ▶ In the **Private** text box, enter the v1.6 device private community string.

The default value is public in both the **Public** and **Private** fields.
- 10 Click **OK** to add the device.
- 11 Test by selecting the newly added device. Right-click on the device name and select **Query** from the drop-down options. Verify that the device is successfully queried from the server.
- 12 After a successful query, right-click and select **Install**.
- 13 Verify that the buttons appear on the device.

Choosing an authentication method

The AccuRoute Embedded Device Client must be able to authenticate the device user when the **Personal Distributions** or **Scan to My Files** options are used.

You can configure:

- LDAP authentication
- AccuRoute authentication at the device

Note HP Pro devices do not support LDAP authentication.

Configuring LDAP authentication

When you choose LDAP Authentication, the user is prompted to enter an email username and password. The Authentication Manager uses the login credentials to initiate a lookup. The lookup validates the user and returns the user's email address. Then the AccuRoute Embedded Device Client uses the email address to request information from the AccuRoute server, such as a list of the user's Personal Distributions. When the scan is submitted to the AccuRoute server as a message, the email address is used to set the property prOriginator.

Both the email username and password are required to identify the device user, and the credentials are validated via LDAP authentication. This method provides increased security.

Note With **LDAP Authentication** configured for the device group on the Administrator, the LDAP lookup only appears on the device once **Require Authentication** is enabled for the relevant device button. See step 6 in [Defining Password Properties \(7-9\)](#) for details.

Section 7: Required Configuration

The following figure is an example of an LDAP Authentication configuration for Active Directory. (For information on configuring LDAP Authentication, consult [AccuRoute v4.1 Documentation](#).)

Figure 7-1: Example of an LDAP authentication configuration for Active Directory (2 screens)

LDAP Authentication binds to the LDAP server with the device user's common name (CN). The search is conducted within the root ou=engineering,cn=users,dc=hp,dc=com using the device user's common name (CN). The return value is the user's email address (mail) and name (displayName)

Control Panel Application	Device Guest	Device Administrator	Device User	Sign In Method
Fax application	Requires Sign In	Full Access	Full Access	Local Device
E-mail application	Requires Sign In	Full Access	Full Access	Use Default
Address Book	Requires Sign In	Full Access	Full Access	Use Default
Save to USB application	Requires Sign In	Full Access	Full Access	Use Default
Save to SharePoint	Requires Sign In	Full Access	Full Access	Use Default
Network Folder application	Requires Sign In	Full Access	Full Access	Use Default
Job Status application	Requires Sign In	Full Access	Full Access	Use Default
Administration application	Requires Sign In	Full Access	Full Access	Use Default
Device Maintenance application	Full Access	Full Access	Full Access	Use Default
Public Distributions	Full Access	Full Access	Full Access	Use Default
Personal Distributions	Requires Sign In	Full Access	Full Access	LDAP
Fax	Full Access	Full Access	Full Access	Use Default
Routing Sheet	Full Access	Full Access	Full Access	Use Default
MyAccuRoute	Requires Sign In	Full Access	Full Access	LDAP
Scan To Folder	Full Access	Full Access	Full Access	Use Default

Allow users to choose alternate sign-in methods
 Automatically sign users out after starting each job

Configuring AccuRoute authentication on the device

- 1 Open a Web browser and enter the device IP address.
- 2 Log in to the Embedded Web Server. All options become available.

3 Go the **Settings** tab and click **Authentication Manager**.

4 Locate the following AccuRoute functions:

- ▶ Scan to My Files
- ▶ Personal Distributions
- ▶ Scan to Me

The list shows the options that are installed with AccuRoute Embedded Device Client, so it can contain all, some, or none of these functions.

5 For each of the features listed above, click on the drop-down menu.

6 Select **LDAP** as the authentication method for each scanning feature that requires user login.

Authentication Manager

Set the Device Functions that require users to successfully sign in before use. Each function can require a different Sign In Method.

Home Screen Access	Sign In Method
Sign In At Walk Up	None
Device Functions	Sign In Method
Copy	None
Color Copy	None
Send to E-mail	None
Send Fax	None
Send to Folder	None
Job Storage	None
Create Stored Job	None
Digital Sending Service (DSS) Secondary E-mail	None
Digital Sending Service (DSS) Workflow	None
Simplex Copy	None
Public Distributions	None
Personal Distributions	None
Fax	None
Routing Sheet	None
Scan To Me	LDAP
Scan To Folder	None
HP AC Express	HPAC - PIC Server
Scan To My Files	LDAP
Future Installations	Sign In Method

7 Click **Apply**.

Configuring the server

When a message arrives on the AccuRoute server, the Dispatch component applies rules to the message. The rules determine how the server processes the message. Every message on the server must match a rule associated with an action in order to be processed and distributed to its final destination. The additional configuration in this section ensures that rules exist for AccuRoute scanning features.

Several AccuRoute scanning features require special rules on the AccuRoute server. Most of these rules are created by default when you install AccuRoute. You can, if needed, create rules based on the AccuRoute scanning features available on devices in your environment. For more information on rules and how to create them, refer to the [AccuRoute server administrator on-line help](#).

When rules have been created for all AccuRoute scanning features available on devices in your environment, the AccuRoute server is fully configured for the AccuRoute Embedded Device Client. Now you are ready to test the AccuRoute scanning features. Continue with the information in [Section 10: Testing](#) (10-77).

Section 8: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

The information in this section will allow you to administrate and install AccuRoute Embedded Device Client buttons onto HP devices using the Web Jetadmin application. This section includes:

[Supported Devices](#) (8-1)

[Exporting the XML files](#) (8-2)

[Installing AccuRoute Embedded Device Client buttons](#) (8-5)

Supported Devices

The following devices are supported:

Table 8-1: AccuRoute Embedded Device Series Matrix

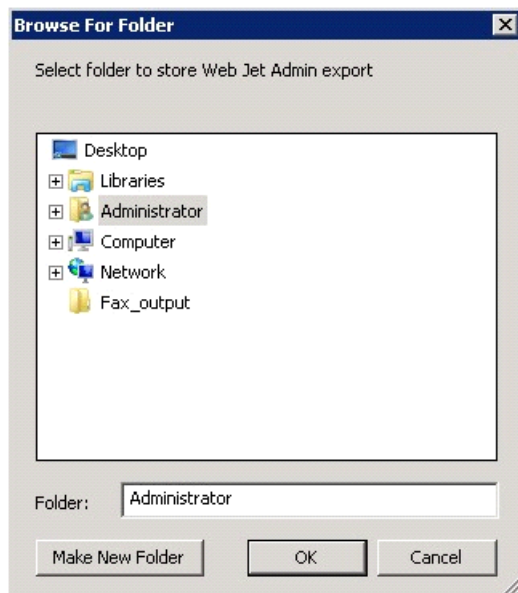
Device	Operating System	Device	Operating System
Color LaserJet CM 4730 MFP	Oz	Color LaserJet CM 6049 MFP	Oz
Digital Sender 9250c	Oz	Color LaserJet CM 3530 MFP	Oz
LaserJet M3035 MFP	Oz	Color LaserJet CM 4540 MFP	FutureSmart
LaserJet M4345 MFP	Oz	ScanJet 7000n	FutureSmart
LaserJet M4349 MFP	Oz	ScanJet 8500	FutureSmart
LaserJet M5035 MFP	Oz	LaserJet Flow M525 MXP	FutureSmart
LaserJet M5039 MFP	Oz	LaserJet Flow M575 MXP	FutureSmart
LaserJet M9040 MFP	Oz	LaserJet M775 MFP	FutureSmart
LaserJet M9050 MFP	Oz	LaserJet M4555 MFP	FutureSmart
LaserJet M9059 MFP	Oz	HP Color LaserJet Flow M880	FutureSmart
Color LaserJet CM 6030 MFP	Oz	HP Color LaserJet Flow M830	FutureSmart
Color LaserJet CM 6040 MFP	Oz	HP LaserJet MFP M725	FutureSmart

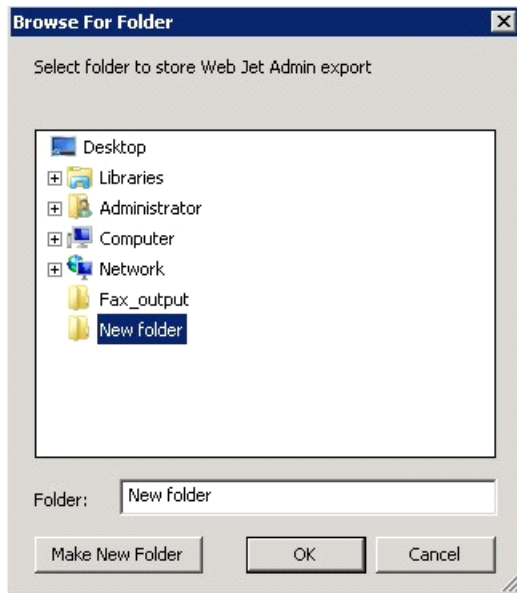
Exporting the XML files

Complete the following procedure for AccuRoute to configure the AccuRoute Embedded Device Client with the appropriate settings for your environment.

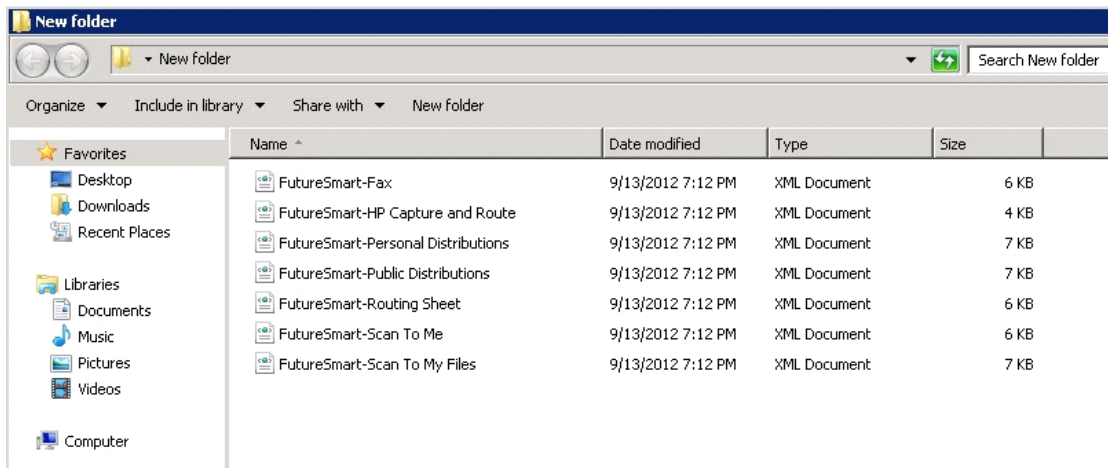
- 1 Once the configuration is complete (as described in [Section 3: Installation](#) and [Section 7: Required Configuration](#)), right-click the **Devices** group to which you intend to deploy buttons. Select **Export to Web Jet Admin**.
- 2 You can now store the XML files by browsing to a network folder or creating a new folder destination.

Browse:



Make New Folder:

- 3 Click **OK** and verify the correct buttons are represented in XML format.



Manually importing a certificate

For HTTPS support, you need to import the client certificate into the device Embedded Web Server (EWS) before installation, as follows:

- 1 Save the certificate to be used for HTTPS communication to a network-accessible location.
- 2 Open and log into the EWS of the device.
- 3 In the **Security** tab, select **Certificate Management**.
- 4 Under **Certificates**, select **Choose File > Browse**.

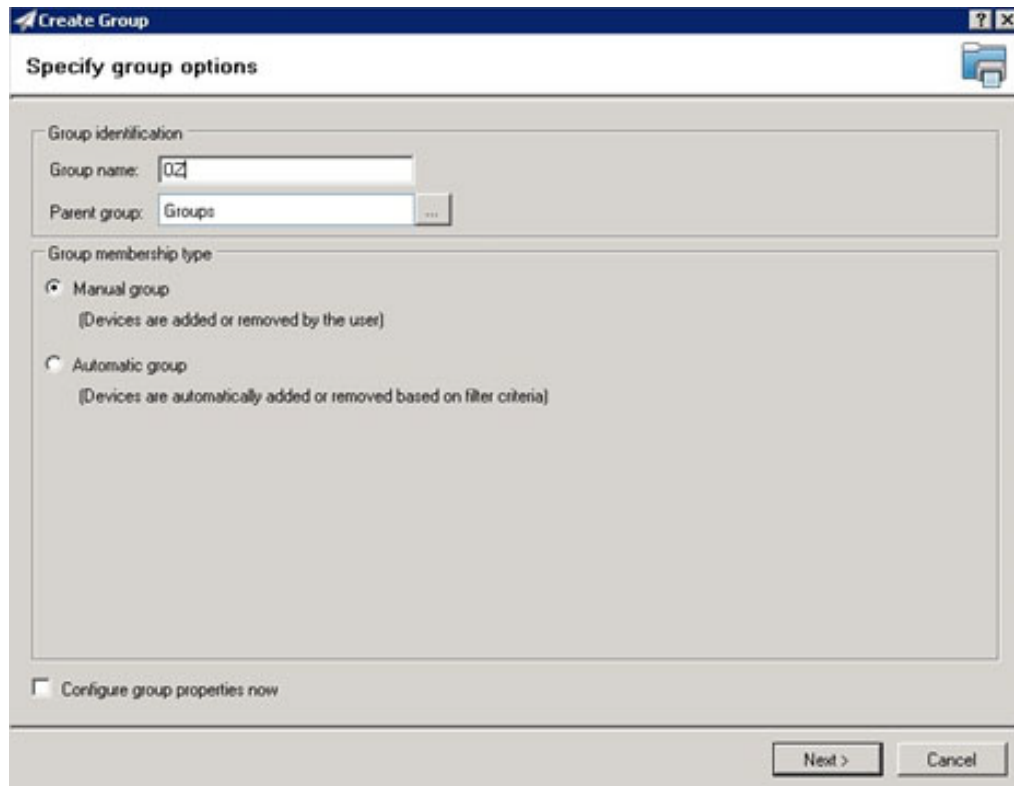
- 5 Browse to the location where you saved the certificate and select **Open > Import**.
- 6 Verify that the certificate appears under the **Certificates** section within the device Embedded Web Server.

Installing AccuRoute Embedded Device Client buttons

Once you can discover devices using the Web Jetadmin application, you can install the buttons using the Web Jetadmin application.

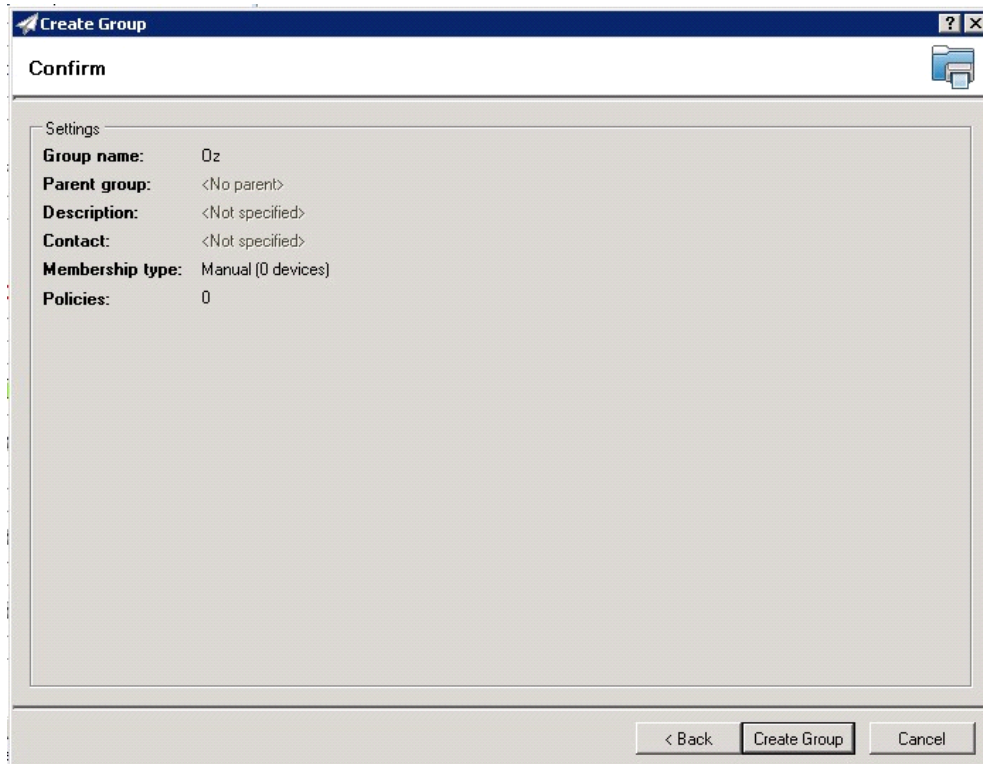
- 1 Right-click the **Group** node and select **New group**.

The **Specify group options** page is displayed.

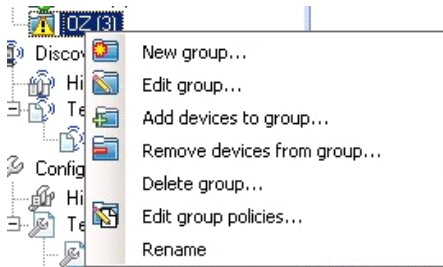


- 2 Enter the name of the new group that you will use to group similar devices for button installation. (Preferably, this is a device group name that will allow the administrator to easily configure similar firmware or button functionality installations such as Jedi, Oz, etc.)

- 3 Click **Next** and verify the group name is correct. The **Confirm** page appears, showing the settings for the group.

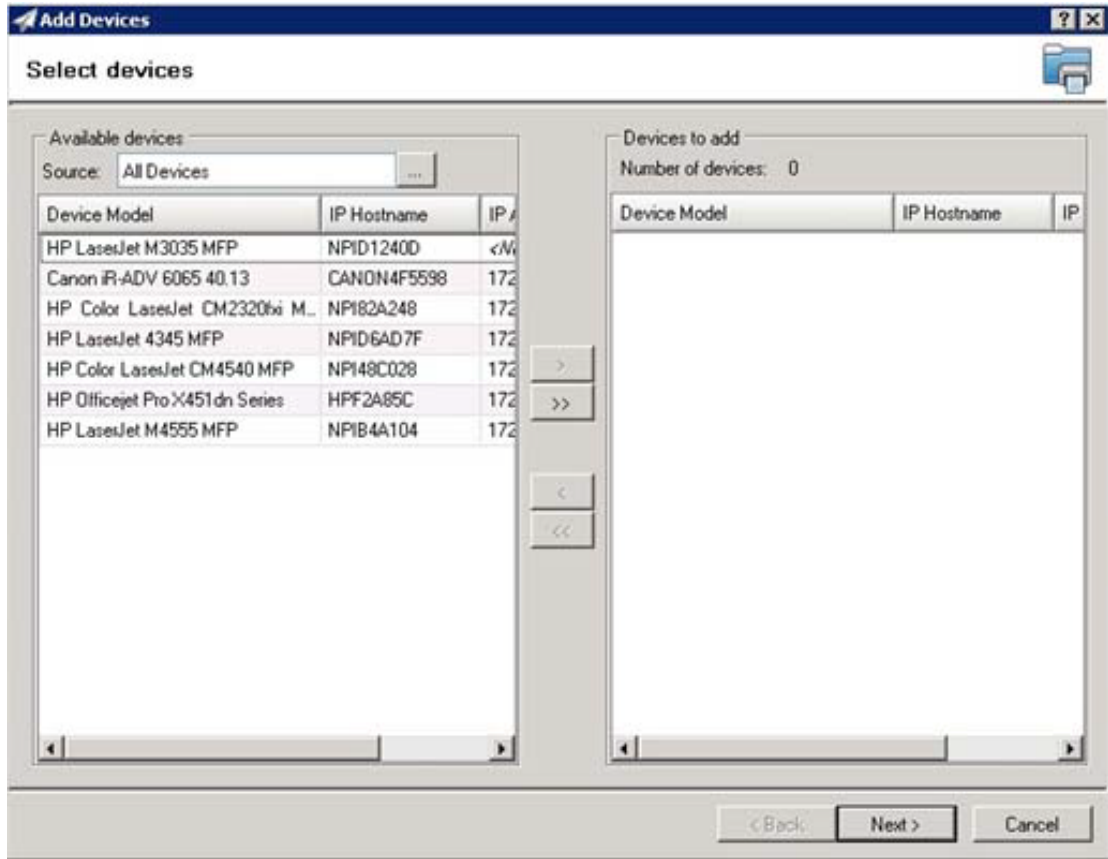


- 4 Click **Create Group** and then **Done**.
- 5 Right-click the newly created group and select **Add devices to your group**.



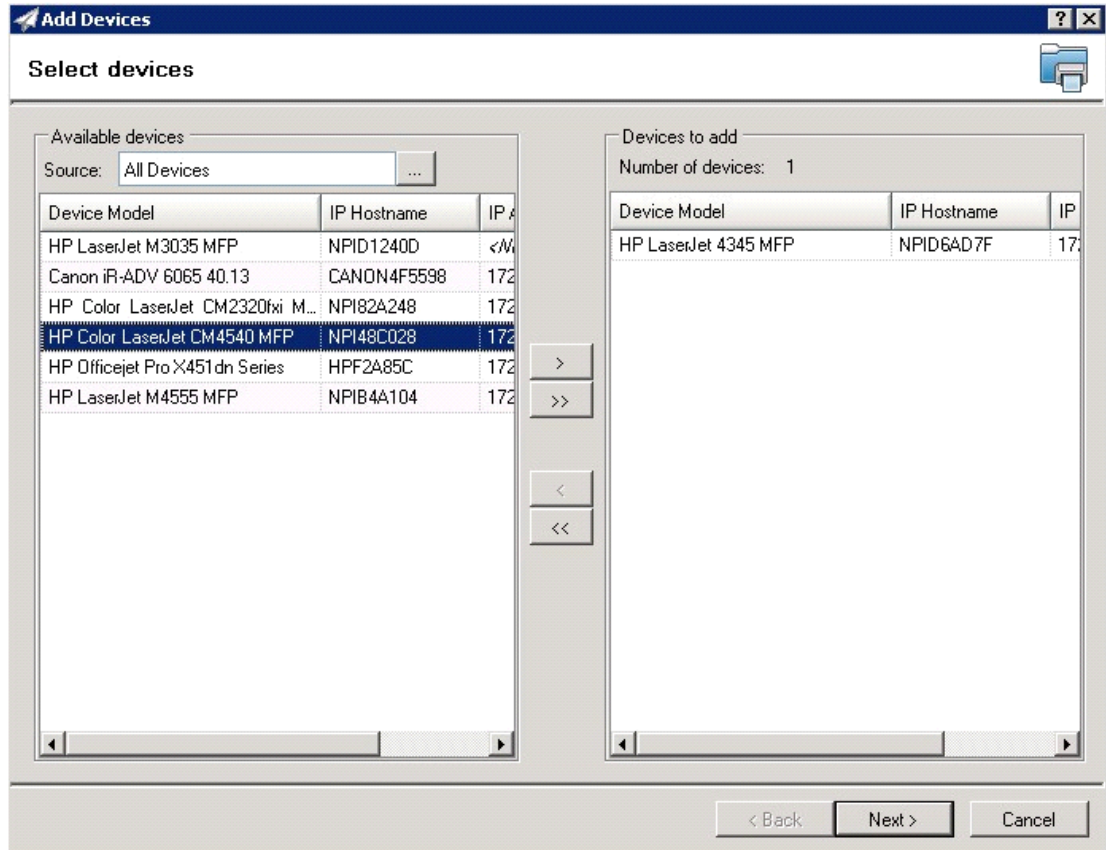
Note For more options to use the Web Jetadmin device filters to find or add devices, consult Omtool's Web Jetadmin team for a complete Web Jetadmin installation guide.

The **Select Devices** page appears.

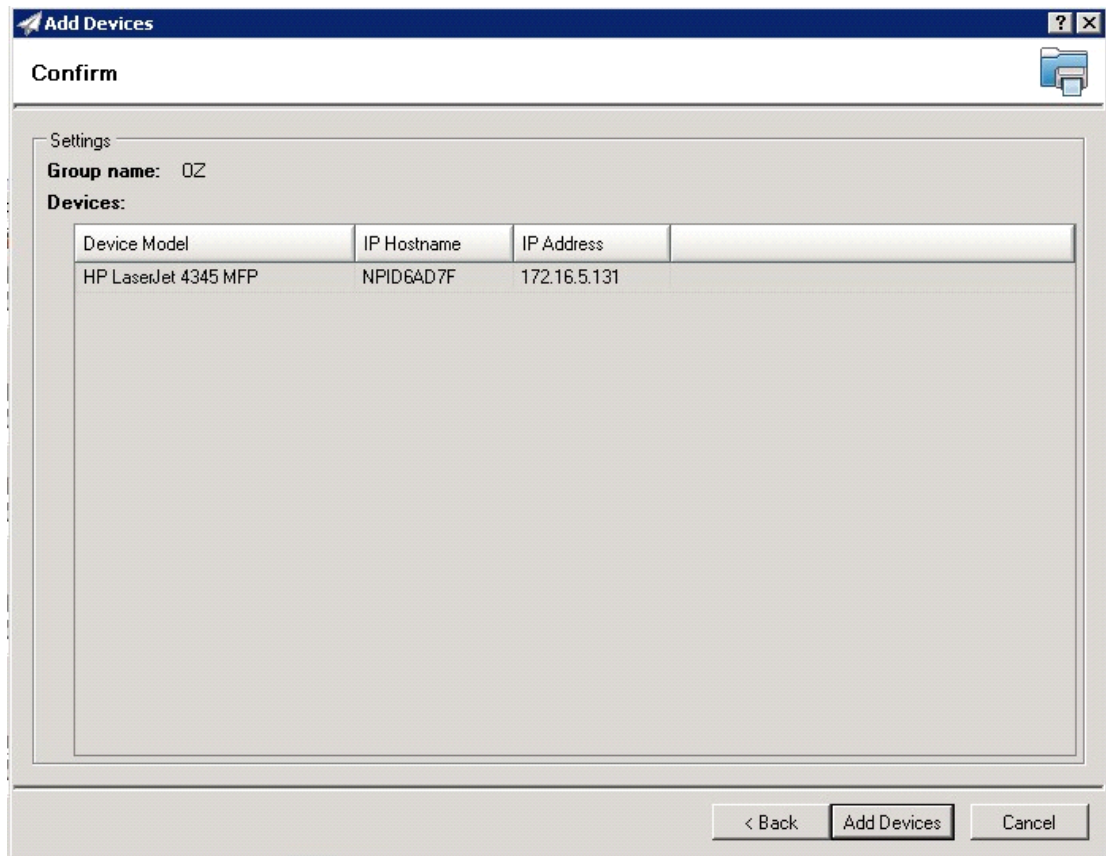


Section 8: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

- 6 In the **Available devices** list (on the left), highlight the device(s) to be added to the group. Then click the > (add) button. The selected device(s) are added to the **Devices to add** list (on the right).



- 7 Click **Next**. The **Confirm** page appears.



The screenshot shows a web browser window titled "Add Devices" with a "Confirm" sub-header. Below the header, there is a "Settings" section with "Group name: OZ". Underneath is a "Devices:" section containing a table with the following data:

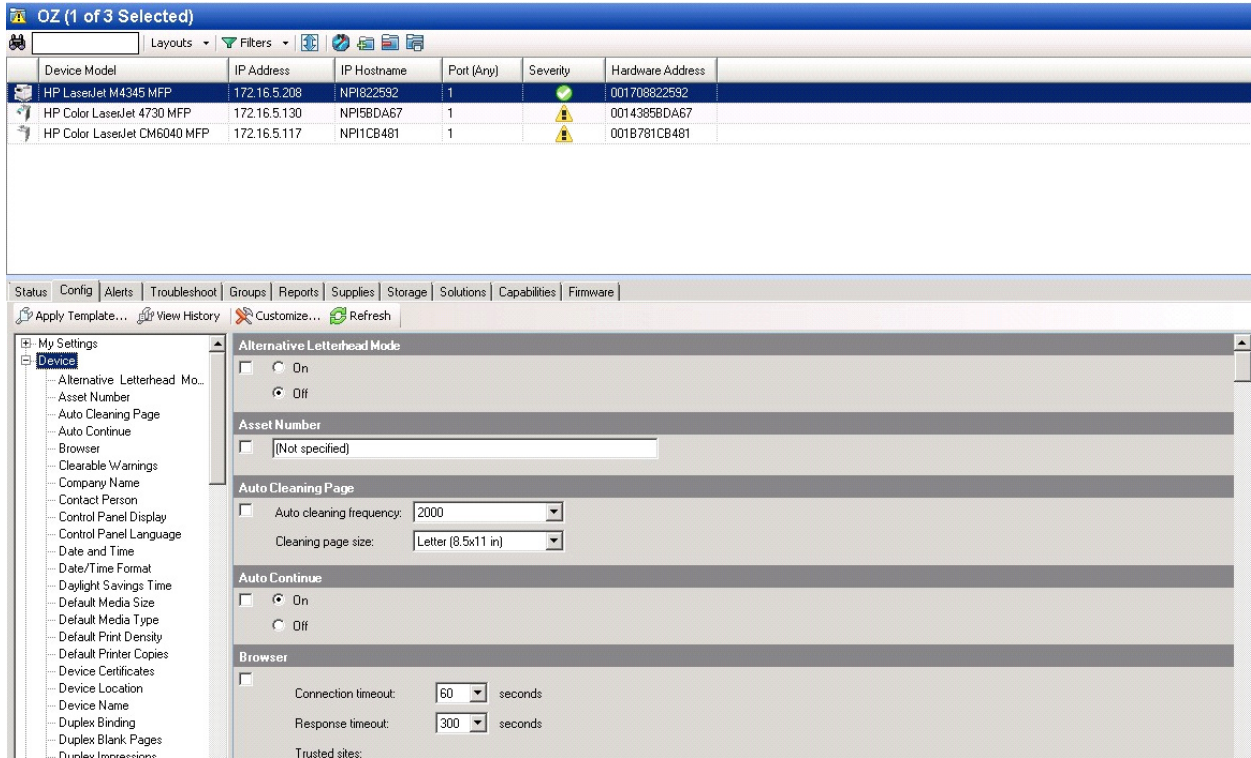
Device Model	IP Hostname	IP Address
HP LaserJet 4345 MFP	NPID6AD7F	172.16.5.131

At the bottom of the window, there are three buttons: "< Back", "Add Devices", and "Cancel".

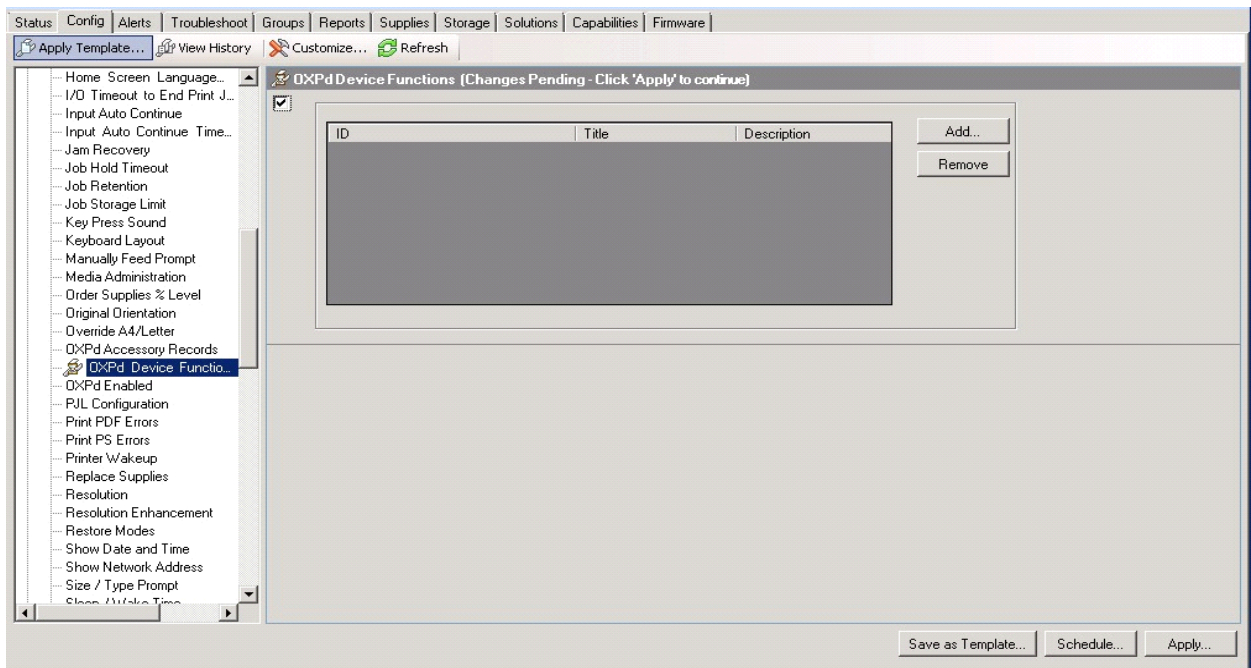
- 8 Click the **Add Devices** button. You should see the devices added to your new group in the **Group** window.

Section 8: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

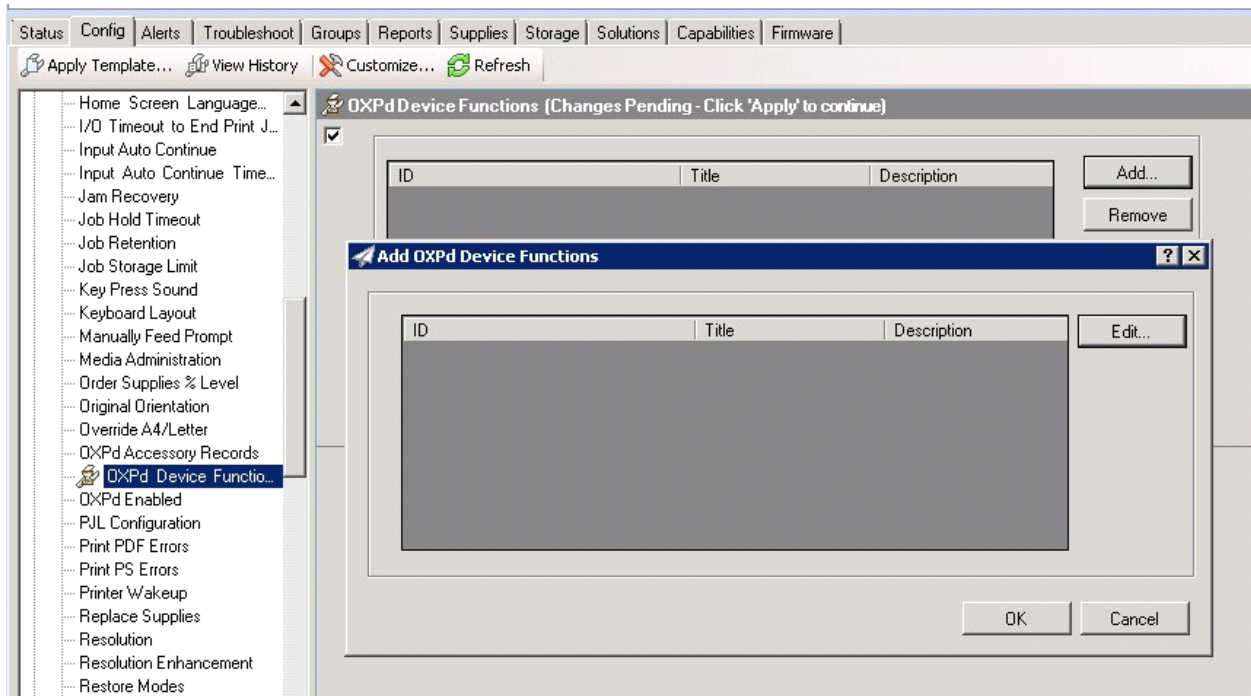
9 Highlight the device(s) to which you want to install buttons.



10 Click the **Config** tab and scroll to the **Embedded Device Functions** subset (as shown below) and check the box in the upper left corner of the center window. The title bar of that area will display: *Embedded Device Functions (Changes Pending - Click 'Apply' to continue).*

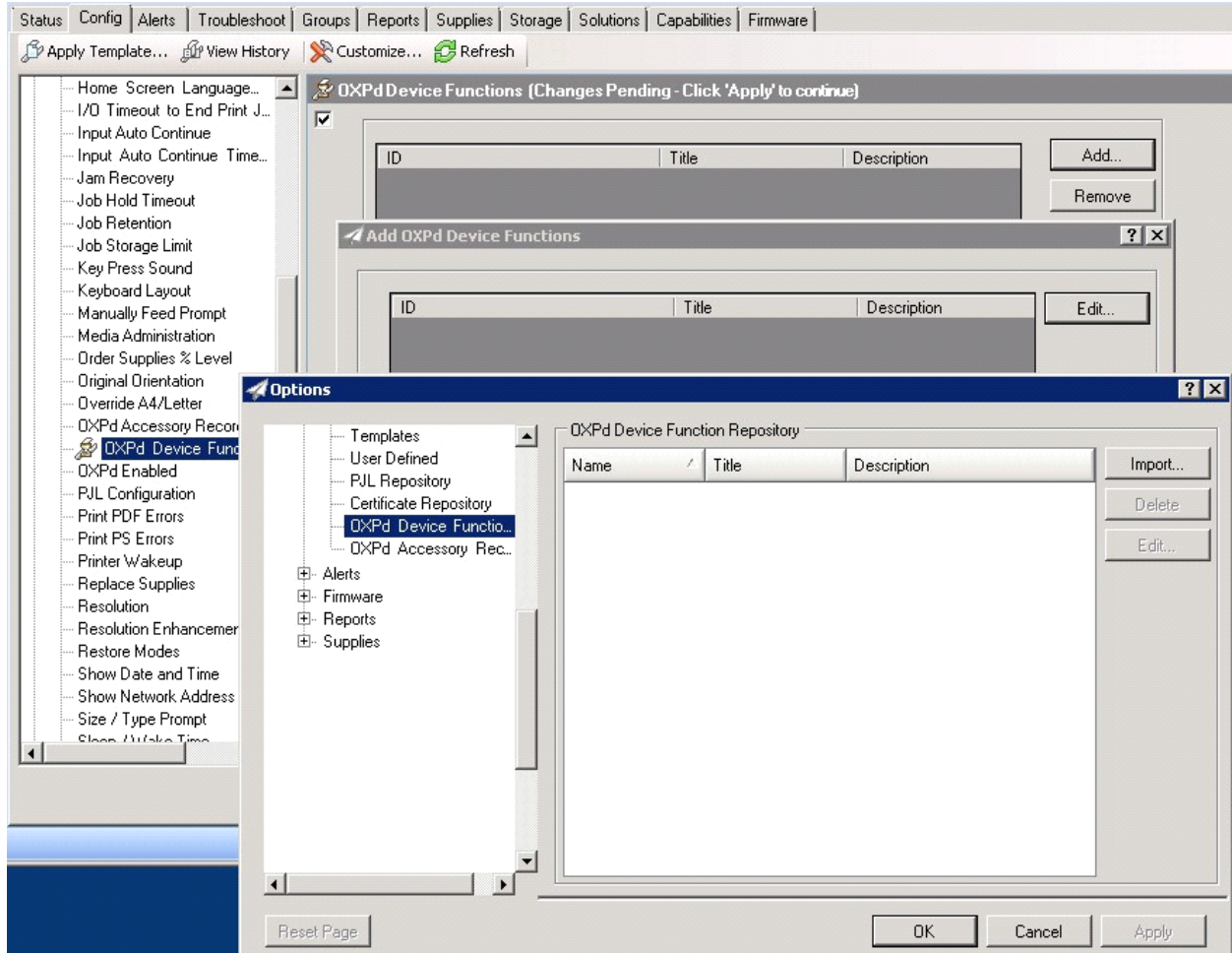


II Click the **Add** button. The **Add Embedded Device Functions** page appears.

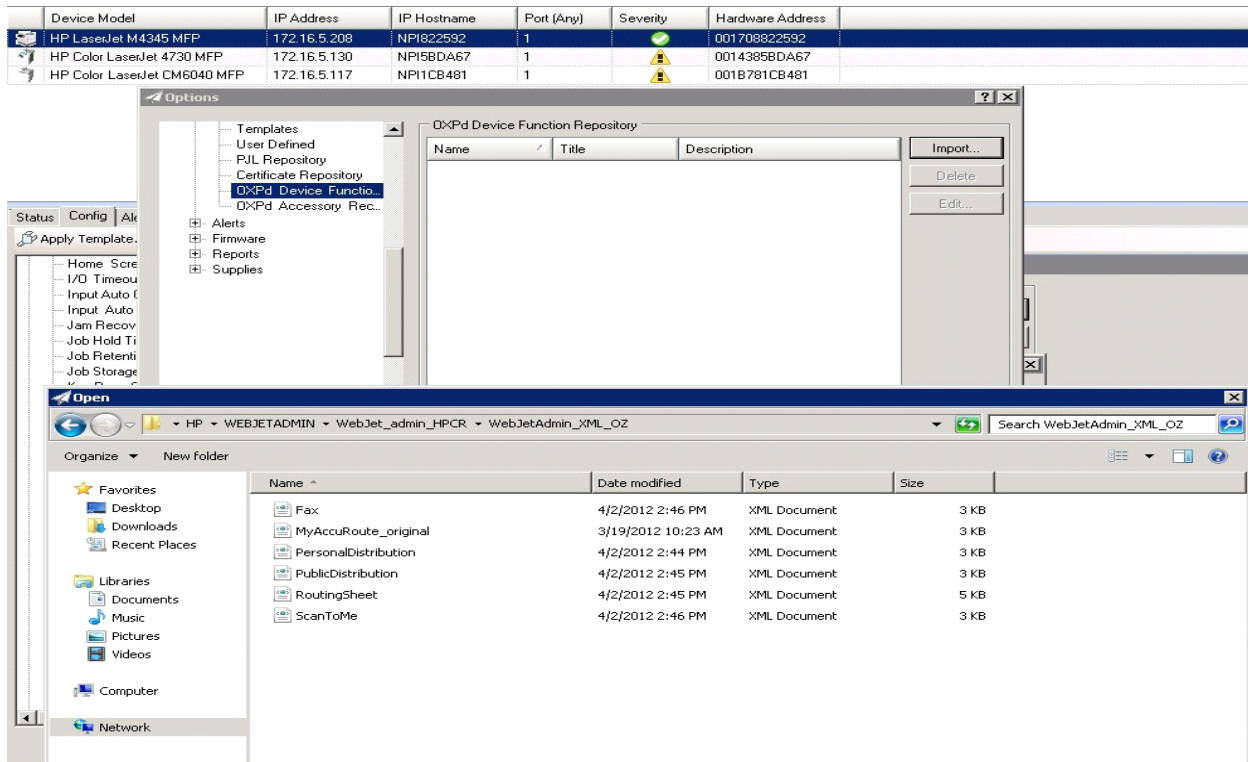


Section 8: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

- 12 Click the **Edit** button. The **Embedded Device Function Repository** page appears and enables you to import the edited Embedded Device solutions XML files (from [Exporting the XML files](#) on page 8-2).

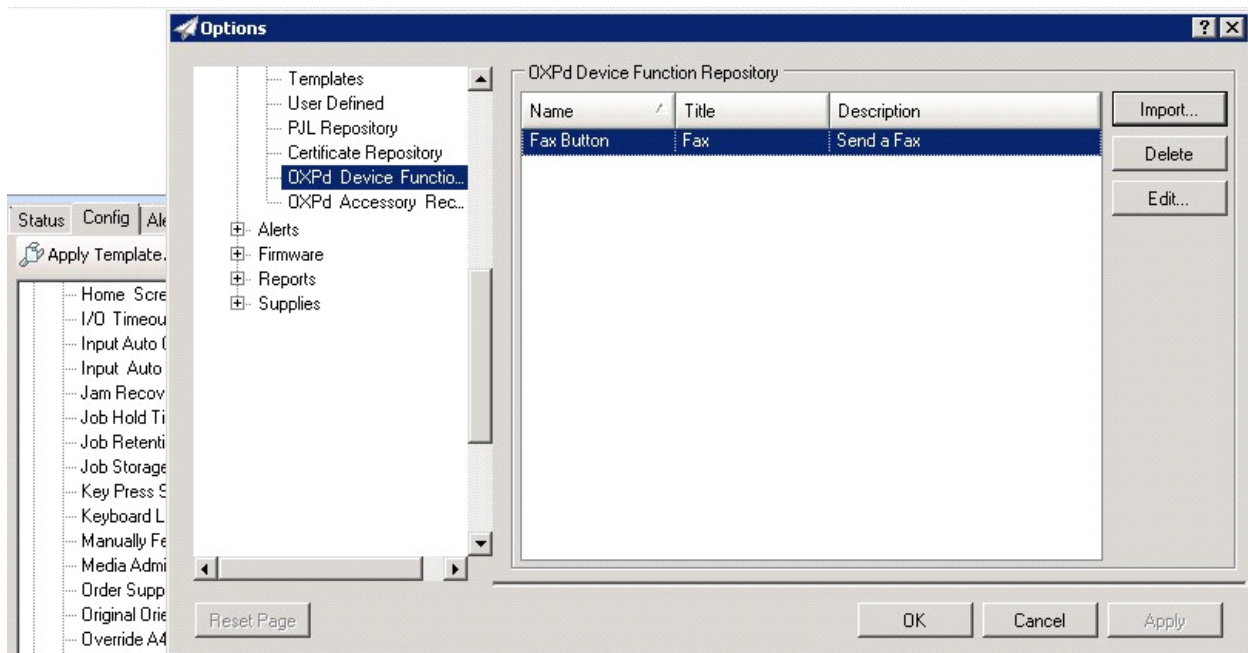


13 Click **Import**. In the **Open** page, search for your XML files.

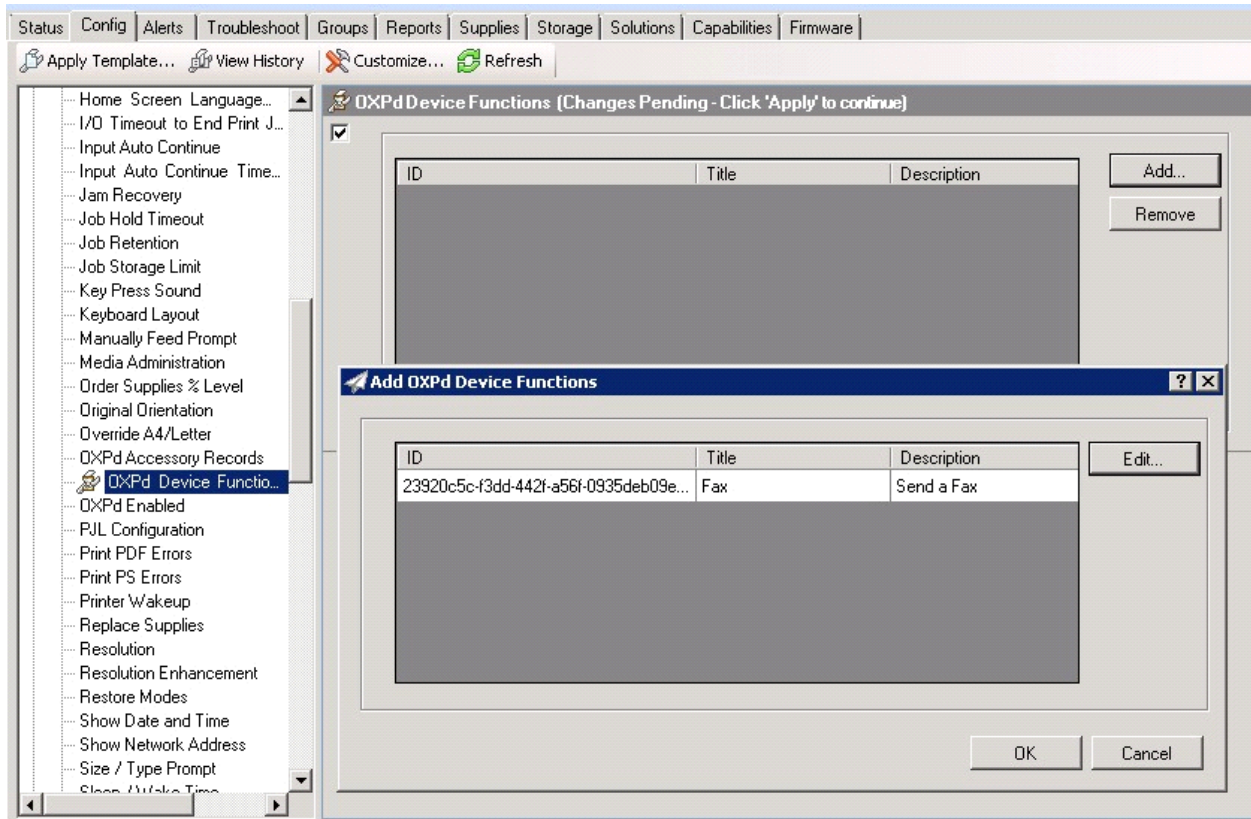


14 Select and highlight the file and then click **Open** to add the file. (You can import only one file at a time in the **Open** window.)

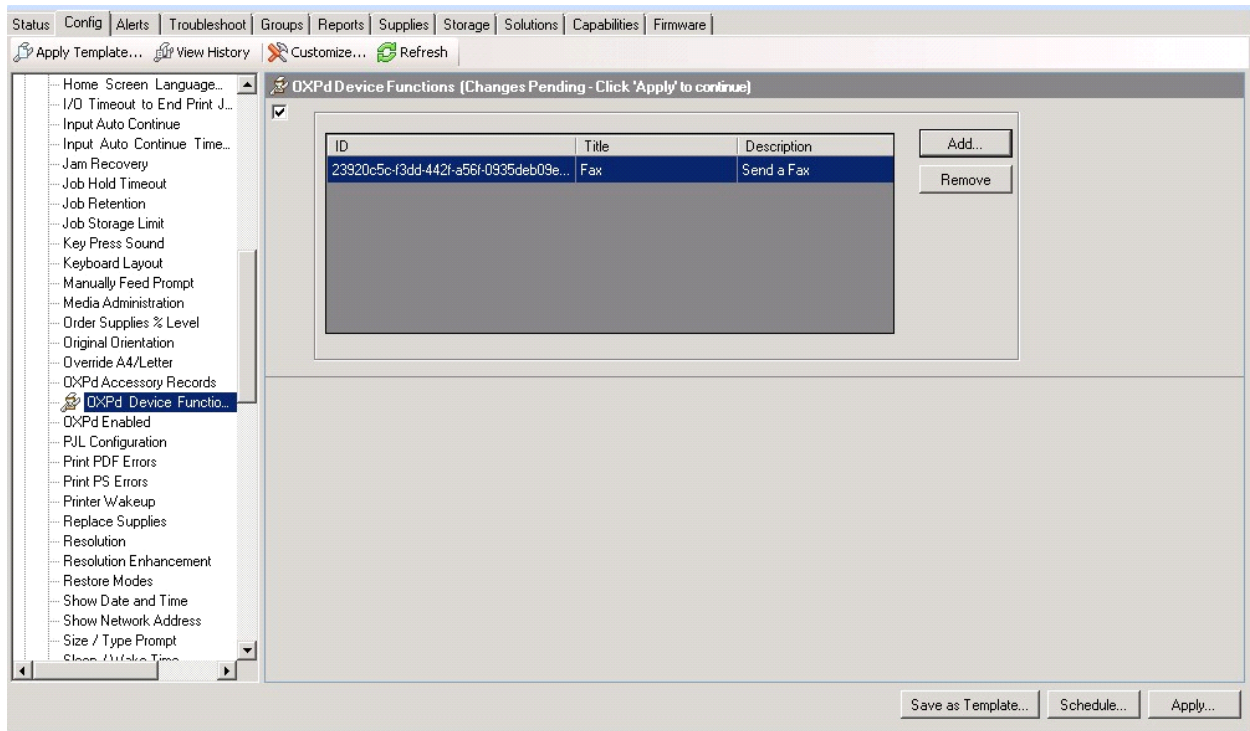
15 Verify that the selected feature XML file is reflected in the **Embedded Device Function Repository** page.



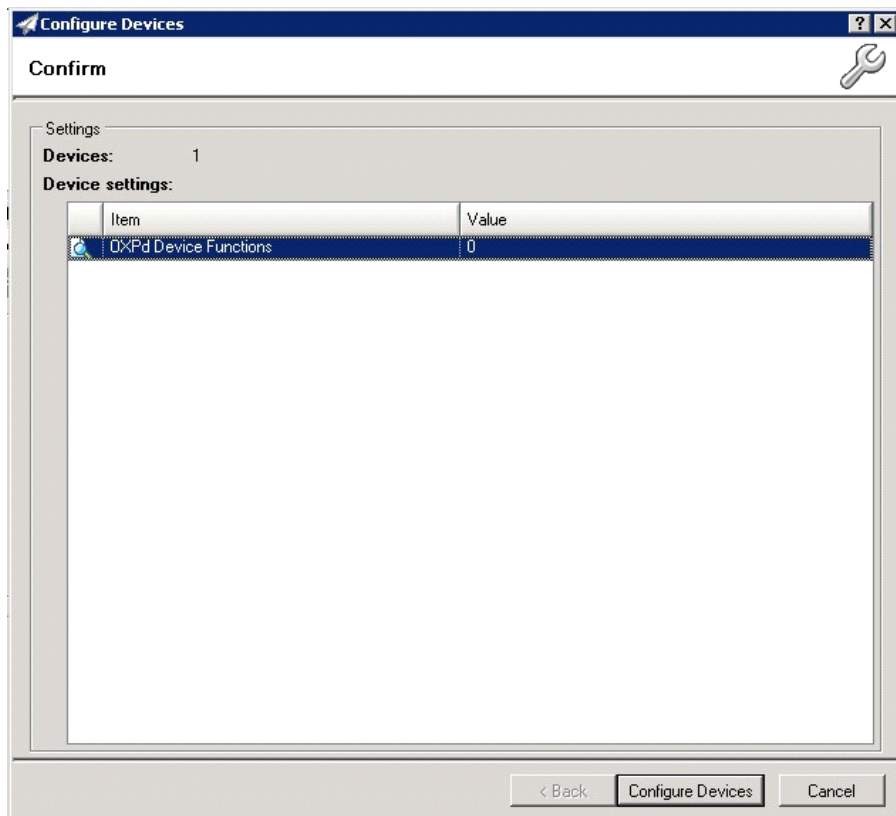
Section 8: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

16 Click OK. The Add Embedded Device Functions page appears.**17 You should see the file referring to the feature(s) or button(s) you are about to install onto the device. Click OK to close the Add Embedded Device Functions page and return to the Embedded Device Functions winpagedow.**

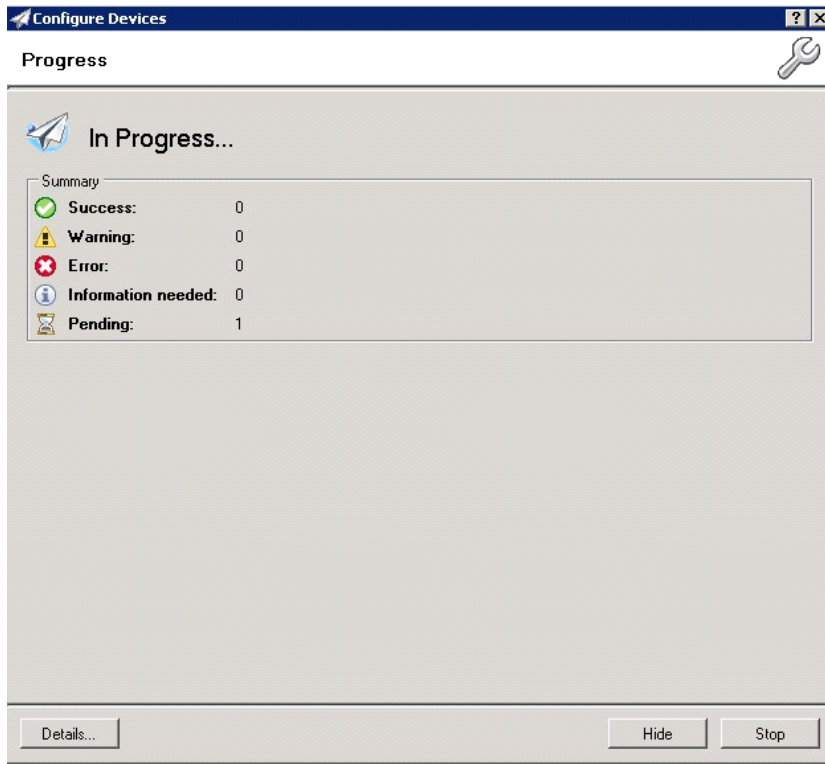
At this point, you can continue to add another feature or button (repeating Steps 11 through 16).



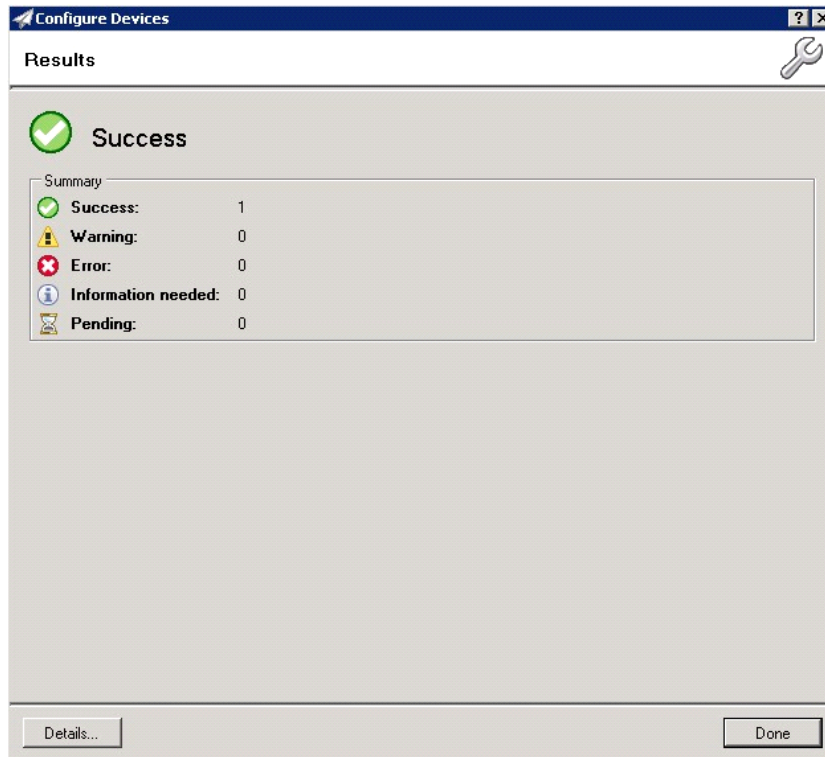
- 18 After you have added and confirmed all of the features/buttons of interest, click **Apply**. **Confirm** page appears.



19 Click the **Configure Devices** button. The **In Progress** page appears.



The **Results** page indicates whether the installation was successful or an error was received.



Note You can click the **Details** button to show additional notes if an error has occurred.

20 Click **Done** to return to the main **Group** page, which defaults to the **Device** subset node.

The screenshot displays the Web Jetadmin interface. At the top, a blue header bar shows 'OZ (1 of 3 Selected)'. Below it is a table with columns: Device Model, IP Address, IP Hostname, Port (Any), Severity, and Hardware Address. The table contains three rows of device information. Below the table is a navigation menu with options like Config, Alerts, Troubleshoot, Groups, Reports, Supplies, Storage, Solutions, Capabilities, and Firmware. The main area shows a configuration panel for 'Alternative Letterhead Mode' with various settings like 'On/Off', 'Asset Number', 'Auto Cleaning Page', 'Auto Continue', and 'Browser'.

Device Model	IP Address	IP Hostname	Port (Any)	Severity	Hardware Address
HP LaserJet M4345 MFP	172.16.5.208	NPI822592	1		001708922592
HP Color LaserJet 4730 MFP	172.16.5.130	NPI5BDA67	1		0014385BDA67
HP Color LaserJet CM6040 MFP	172.16.5.117	NPI1CB481	1		001B781CB481

Alternative Letterhead Mode

On
 Off

Asset Number

Auto Cleaning Page
 Auto cleaning frequency: 2000
 Cleaning page size: Letter (8.5x11 in)

Auto Continue
 On
 Off

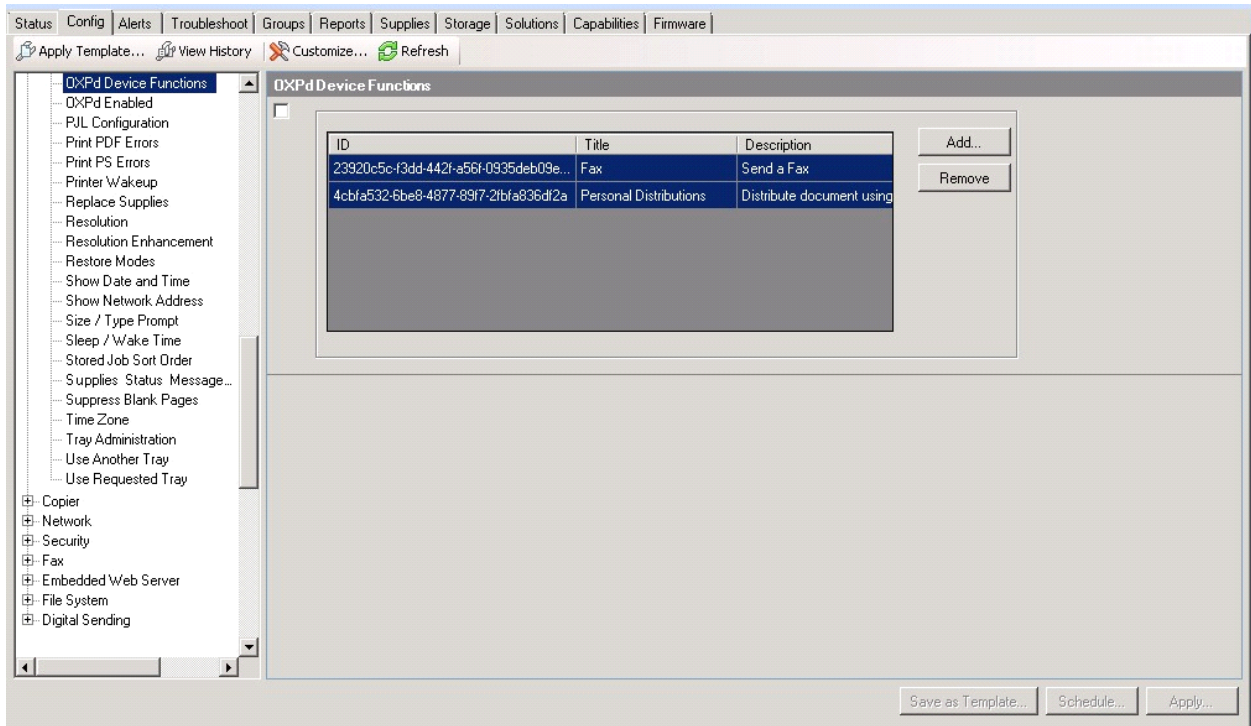
Browser
 Connection timeout: 60 seconds
 Response timeout: 300 seconds
 Trusted sites:

Use semicolons(;) to separate addresses

Save as Template... Schedule... Apply...

Section 8: Using the Web Jetadmin Application to Install Embedded Device Client Buttons on HP Devices

21 Scroll down to the **Embedded Device Functions** subset and you should see the feature buttons that were successfully added to the HP device.



22 Test the buttons on the device panel to verify all functionality.

Section 9: Testing

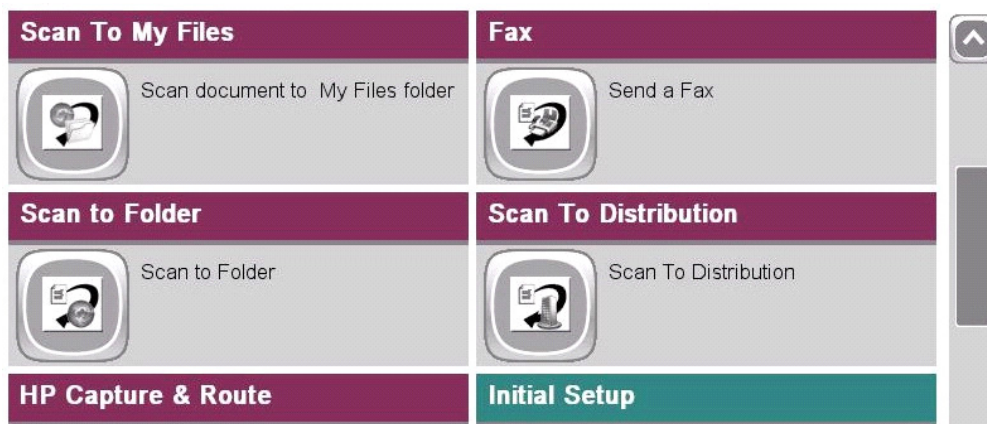
The following section provides a procedure for testing the Routing Sheet feature. This will ensure that your installation is operational. This section includes:

[Testing the Routing Sheet feature](#) (9-1)

[Testing the Device Administrator user interface](#) (9-2)

Testing the Routing Sheet feature

- 1 Create at least one Distribution Rule with your user account.
- 2 Generate and print a Routing Sheet using the AccuRoute Desktop or the AccuRoute Web Client application.
- 3 Assemble a test document. Add the Routing Sheet to the front of the document and go to the device. The main screen looks like this:



- 4 Load the document into the document feeder.
- 5 Press **Routing Sheet**. (If this feature is not visible, use the scroll bar to find it.)

Note If you have configured prompts, you will see the them now. Enter the appropriate prompt values and click **Next**.

The device indicates it is ready to scan.

- 6 To begin scanning, press **Start** on the display screen or on the hard keypad.


Alternately, to change the scan attributes, click **More Options**.

For example, you can specify the page size for the scanned document. The default page size is Letter. After you have made your modifications, click **Start** to begin scanning.

The scan job starts. A progress indicator shows the scan job status

To stop the scan job, press **Cancel Job**. Otherwise wait for the job to finish. When scanning is complete, the device shows the scan completed message.

The message is transferred to the AccuRoute server via HTTP/HTTPS where it is processed and routed to the intended recipient. If the document does not arrive at the destination, troubleshoot the setup. Go to [Section 10: Troubleshooting](#).

- 7 To scan another document using the Routing Sheet option, click **Back**. To end the session and go back to the main AccuRoute menu, click  or the **OK** button.

Important If you see that the AccuRoute server cannot decipher or interpret the Distribution Rule instructions on the Routing Sheet, you must change the device setting from **mixed** to **text**. For instructions, see [Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet \(10-6\)](#)

Testing the Device Administrator user interface

To test the Device Administrator user interface, complete the procedure for [Creating a group of devices \(part I\) \(7-1\)](#).

You can set up tests to test all authentication types at once by configuring groups on the AccuRoute server, with each group having a different authentication type:

- Email
- Email with Password
- PIN
- PIN with Password
- Login
- Device

Then, test one device by uninstalling and reinstalling from each authentication type group to verify that all authentication types will work at once.

Section 10: Troubleshooting

This section includes:

[Detecting workflow issues](#) (10-2)

[Troubleshooting the delivery mechanism](#) (10-2)

[Troubleshooting messages on the AccuRoute server](#) (10-3)

[Troubleshooting the Web server](#) (10-5)

[Troubleshooting the multifunction device](#) (10-5)

[Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd](#) (10-5)

[Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices \(Omtool ISAPI Web Server Extension\) in a cluster](#) (10-6)

[Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet](#) (10-6)

[Troubleshooting problems associated with applying all additional scan attributes](#) (10-7)

[Troubleshooting problems when scanning large documents](#) (10-7)

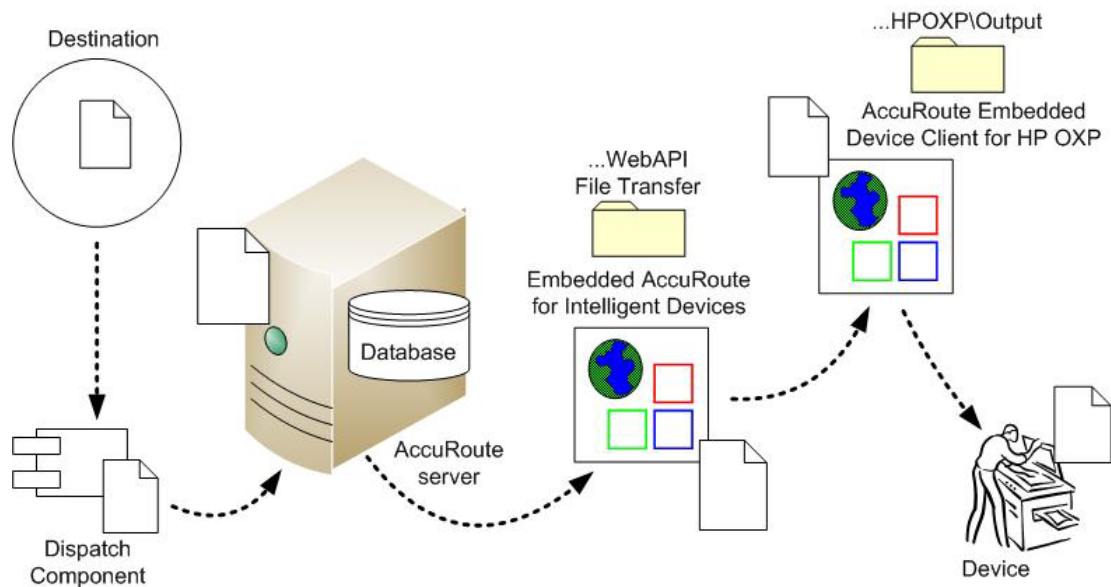
[Troubleshooting problems when scanning 100+ color pages](#) (10-8)

[Troubleshooting an SNMP error](#) (10-9)

If you cannot resolve an issue, contact [Omtool support](#).

Detecting workflow issues

After a document has been scanned on the device, the document should arrive at its destination momentarily but can take up to several minutes when the server workload is high. If a document does not arrive at its destination within a reasonable period of time, begin troubleshooting the environment. Omtool recommends troubleshooting the workflow in reverse order because this is the easiest way to troubleshoot the setup on your own.



When a document does not arrive at its destination, troubleshooting starts with the delivery mechanism such as the mail server or DMS application, and then continues to the AccuRoute server, the AccuRoute Embedded Device Client for HP OXP, the Web server, and the device.

Figure 10-1: Troubleshooting the workflow in reverse order

Troubleshooting the delivery mechanism

When the AccuRoute server finishes processing a message, an outbound connector routes the message directly to its destination or passes the message onto a delivery agent. If a delivery agent such as a mail server or DMS application is involved in the delivery process, do some basic troubleshooting on the delivery agent. If the delivery agent is functioning correctly, troubleshoot the message on the AccuRoute server. Continue to [Troubleshooting messages on the AccuRoute server](#).

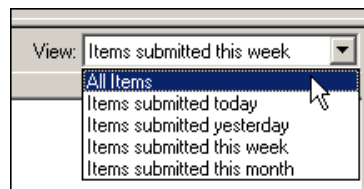
Troubleshooting messages on the AccuRoute server

There are two important questions that can be resolved when troubleshooting a message on the AccuRoute server:

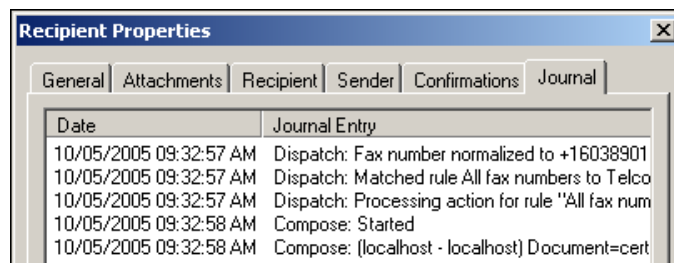
- Was the message submitted to the AccuRoute server?
- Assuming the message was submitted to the AccuRoute server, what caused the delivery failure? The state and status of the message, along with details in the message journal, provide some important clues.

Start troubleshooting by trying to locate the message on the AccuRoute server:

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and go to **[ServerName] > Messages**.
- 3 Look for the message in the In Process queue:
 - a Click **In Process**.
 - b View **All Items**.

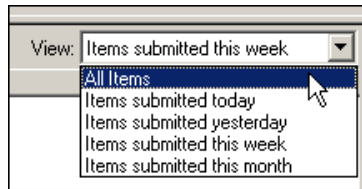


- c Sort all items by the date submitted.
- d Look for the message.
 - ▶ **Message found** - View the message journal to determine the current state and status of the message. Then monitor the components and confirm that the message is moving through the processing queues on the AccuRoute server. If the AccuRoute server stops processing the message (for example, the message seems to be stuck in a processing queue), restart all the Omtool services.

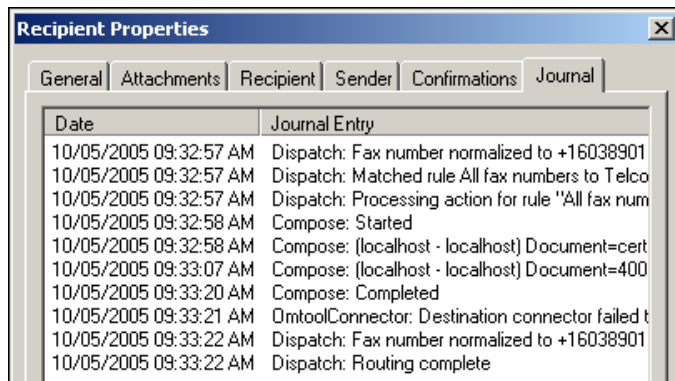


- ▶ **Message not found** - Go to step 4 and look for the message in the History queue.

- 4 Look for the message in the History queue:
 - a Click **History**.
 - b View **All Items**.



- c Sort all items by the date submitted.
- d Look for the message.
 - ▶ **Message found** - View the message journal to determine the cause of the failure.



If the message failed, correct the issue and send the message again. Contact Omttool if you are unable to resolve the issue.

If the journal states that AccuRoute server delivered the message but it still has not arrived at its destination, this indicates that the AccuRoute server transferred the message to the delivery agent successfully. Do some advanced troubleshooting on the delivery agent to determine why the message is not being delivered to its destination. Contact Omttool if you are unable to resolve the issue.

- ▶ **Message not found**

Troubleshooting the Web server

The *Embedded AccuRoute for Intelligent Devices Installation Guide* has instructions on troubleshooting the Web server. For documentation related to AccuRoute v4.0, consult the [AccuRoute v4.0 documentation page](#).

If you cannot identify any issues with the Web server, troubleshoot the device. Continue to [Troubleshooting the multifunction device](#).

Troubleshooting the multifunction device

After troubleshooting all other components in the workflow, troubleshoot the device. Consult the HP documentation.

Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd

Problem:

When installing AccuRoute Embedded Device Client for HP OXPd v1.6 on a Windows 2008 R2 system, this message appears.

```
.NET Framework 3.5.1 must be installed using Server Roles before continuing.
```

Solution:

.NET Framework v3.5.1 is not installed in your system. Install .NET Framework v3.5.1 before proceeding with the AccuRoute Embedded Device Client for HP OXPd v1.6 installation.

For information on how to install .NET Framework v3.5.1, consult:

<http://blogs.msdn.com/b/sqlblog/archive/2010/01/08/how-to-install-net-framework-3-5-sp1-on-windows-server-2008-r2-environments.aspx>

Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster

Problem:

Issues related to permissions occur when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster environment.

Solution:

When setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster, you must configure permissions for the Anonymous user.

Procedures for setting up Embedded AccuRoute for Intelligent Devices in a cluster are provided in the appendix titled, *Setting up an AccuRoute server cluster*, in the [AccuRoute v4.0 Server Installation Guide](#).

Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet

Problem:

When using an HP device to scan a document with a Routing Sheet, the AccuRoute server cannot decipher the instructions on the Routing Sheet and process the document.

Solution:

Change the device setting from scanning a Mixed document to scanning a Text document. To do so:

- 1 Open a Web browser and enter the IP address of the device.
- 2 Click **Log In** and login to the device using the device administrator name and password.
- 3 Click **Digital Sending > Preferences**.
- 4 For **Document Type**, change the chosen option from **mixed** to **text**.

Troubleshooting problems associated with applying all additional scan attributes

Problem:

All additional scan attributes are configured together (Darkness, back ground cleanup, contrast, sharpness, Heavy originals), and the following message appears when attempting to scan a document at the HP device:

```
The action cannot be performed because options specified in the configuration file are not supported by this device. Try again on a different device.
```

Solution:

This message is displayed because the scan options are not supported by the device. Consult your HP manual or with your Administrator and find out which scan options are supported for your device model. The list of scan options commented in the configuration file are not supported by all the devices. Only those options that are supported by a particular device model should be un-commented and used.

Troubleshooting problems when scanning large documents

Problem:

After a document is scanned, the message indicating scan completion with delivery information is missing. However, the document is routed to the AccuRoute server for processing.

Solution:

Configure the following:

- Increase the sleep schedule from 10 minutes to the maximum, which is 4 hours
- Increase the inactivity timeout in the device Embedded Web Server to 300 seconds
- Increase the Content length in Internet Information Service Manager (IIS)

To increase the sleep schedule:

- 1 Log in to the Embedded Web Server.
- 2 Select the **General** tab.
- 3 In the left pane, locate **Sleep Schedule**.
- 4 Increase the Sleep Delay to the maximum allowable time: 120 minutes. Click **Apply**.

To increase the inactivity timeout in the device Embedded Web Server:

- 1 Log in to the Embedded Web Server.
- 2 Select the **General** tab.
- 3 In the left pane, locate **Control Panel Administration Menu**.
- 4 In the center pane, expand **Administration**.

- 5 Click on **Display Settings**.
- 6 Locate **Inactivity Timeout** and increase the value to 300 seconds.

To increase content length in IIS:

Note The content length must be modified on both the OmtoolDXPWebApp1.6 and the OmtoolWebAPI sites.

- 1 Go to the Internet Information Services manager and select **OXPI.6** under **Sites**.
- 2 Double-click on **Request Filtering**.
- 3 Select **Edit Feature Settings** under the **Actions** menu.
- 4 Increase the value in **Maximum allowed content length**. The default value is 30000000. Modify the value to 300000000.
- 5 Select **WebAPI** under **Sites**.
- 6 Double-click on **Request Filtering**.
- 7 Select **Edit Feature Settings** under the **Actions** menu.
- 8 Increase the value in **Maximum allowed content length**. The default value is 30000000. Modify the value to 300000000.
- 9 Reset IIS.

Troubleshooting problems when scanning 100+ color pages

Problem:

When scanning more than 100 color pages, it takes additional time for the scans to arrive on the AccuRoute server.

Solution:

To improve performance.

- 1 Go to the Internet Information Services (IIS) manager configured for AccuRoute 4.0.
- 2 Open the following file for editing (such as with Notepad):
`C:\Program Files (x86)\Omtool\OXPI.6`
- 3 Locate `<httpRuntime maxRequestLength="500000" executionTimeout=1800>`.
Change the executionTimeout to 5400:
`<httpRuntime maxRequestLength="500000" executionTimeout=5400>`
- 4 Save the file and restart IIS.

Troubleshooting an SNMP error

Problem:

When you perform an nvram full init, the Set Community string and the Get Community string are both set to public. However, when you set the admin password, it sets the Set Community string to the admin password. The networking tab of the Embedded Web Server of the device does not display the value if it is set. Instead it shows asterisks (**). The best practice is to set the value to blank, as it will assume public for both and display the value as "Not Set (default to public)."

Solution:

To display the value.

- 1 Log in to the Embedded Web Server.
- 2 Select the **Networking** tab.
- 3 Choose settings under security.
- 4 Under **SNMPc1/2** on the **Status** tab, there are two fields: **Get Community Name** and **Set Community Name**.

Change the community name values by setting the values as blank for **Get Community Name** and **Set Community Name**.

- 5 Click **Apply** to remove any value. Now, no values are set for the two fields.

Appendix A: Configuring HP Pro Devices on a Remote OPS Server with HTTPS Support

This appendix describes the installation and configuration process for HP Pro devices on a remote OPS Server with HTTPS support, which is installed on a system remote from the AccuRoute server. This includes HTTPS support on a remote IIS server.

HP Pro devices require an OPS server for registration prior to installing feature buttons on the devices. The OPS server creates a certificate used for a secure registration of each Pro device. You can also use this certificate in your IIS server for HTTPS support.

This process includes the following steps:

[Installing the AccuRoute Embedded Device Client on the local server](#) (A-1)

[Installing the OPS kit on the remote server](#) (A-2)

[Exporting the OPS server certificate](#) (A-6)

[Importing the OPS certificate into the device EWS](#) (A-7)

[OPS registration](#) (A-7)

[HTTPS support using the OPS-created certificate](#) (A-8)

Note In these steps, *System A* represents the local system. *System B* represents the remote system.

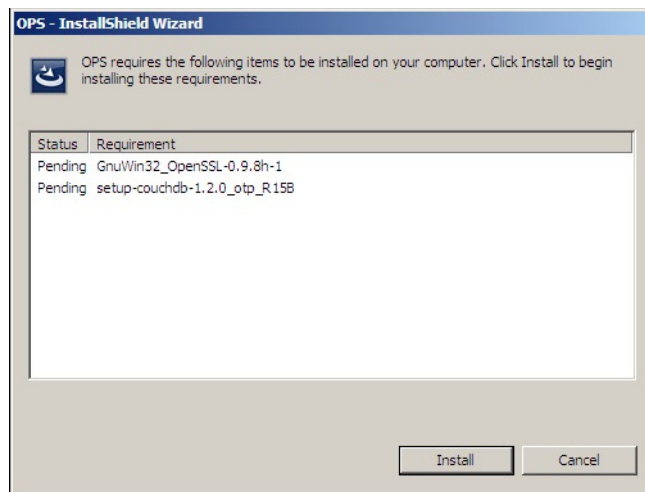
Installing the AccuRoute Embedded Device Client on the local server

On the local system (*System A*) running the AccuRoute server, install the AccuRoute Embedded Device Client. See [Installation](#) (3-1) for more information.

Note If you want HTTPS support with your remote OPS server installation, the OPS server must be installed on the system where the IIS server is installed. To use the HTTPS certificate, the OPS server must be installed on the IIS server.

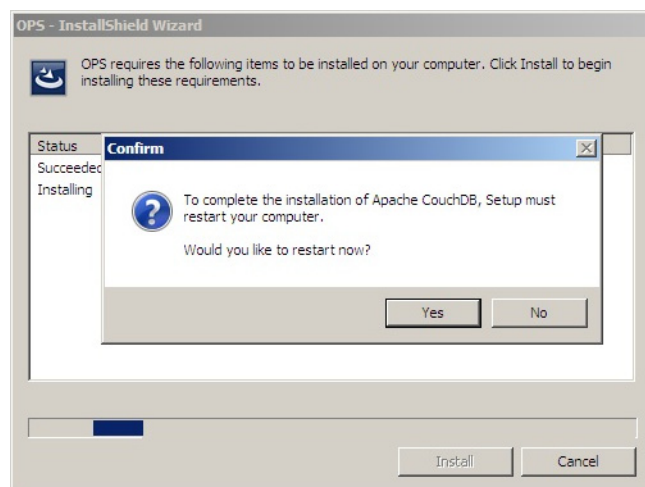
Installing the OPS kit on the remote server

- 1 From the local server (*System A*), navigate to the `\Tools` folder on the remote server (*System B*).
- 2 Right-click and select **Run as Administrator**.
- 3 Run `setup.exe` for OPS on *System B*.
- 4 The OPS InstallShield wizard appears and requests that you install the following two items:
 - ▶ `GnuWin32_OpenSSL-0.9.8h-1`
 - ▶ `setup-couchdb-1.2.0_otp_R15B`



- 5 Click **Install**.
- 6 After installing the items in Step 3, the following message may appear:

To complete the installation of Apache CouchDB, setup must restart your computer. Would you like to restart now?



If this message appears, click **Yes** to restart. The OPS InstallShield wizard reappears upon restarting the system.

Otherwise, the OPS InstallShield wizard **Welcome** screen immediately appears.

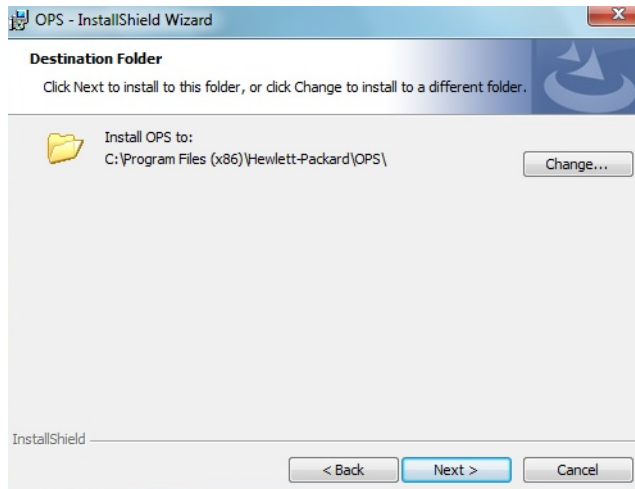


7 Click **Next**. The **License Agreement** screen appears.

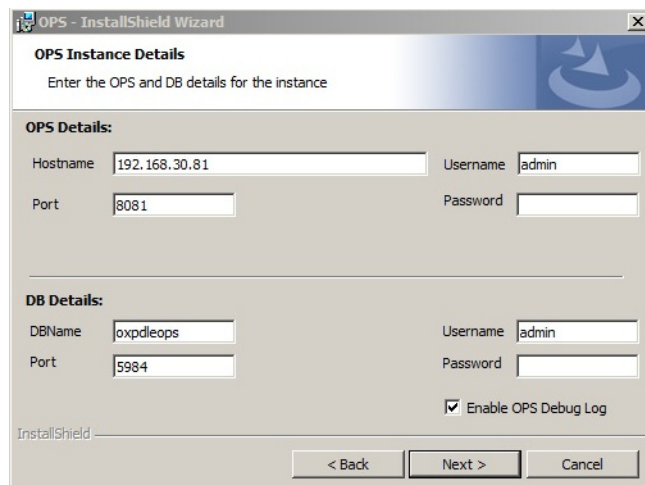


8 Select **I accept the terms in the license agreement** and click **Next**.

The **Destination Folder** screen appears.

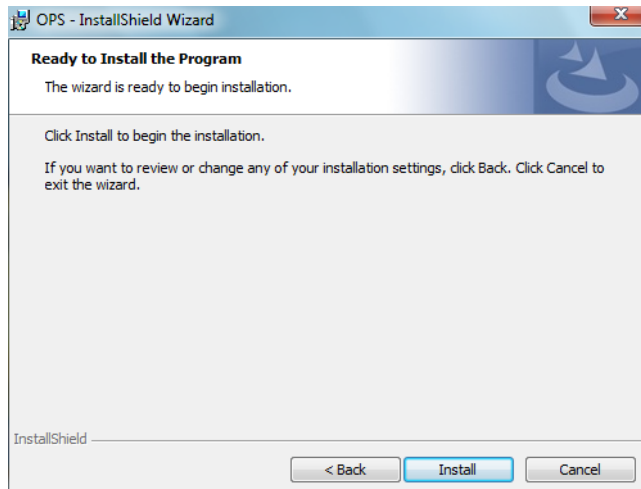


9 Click **Next**. The **OPS Instance Details** screen appears.



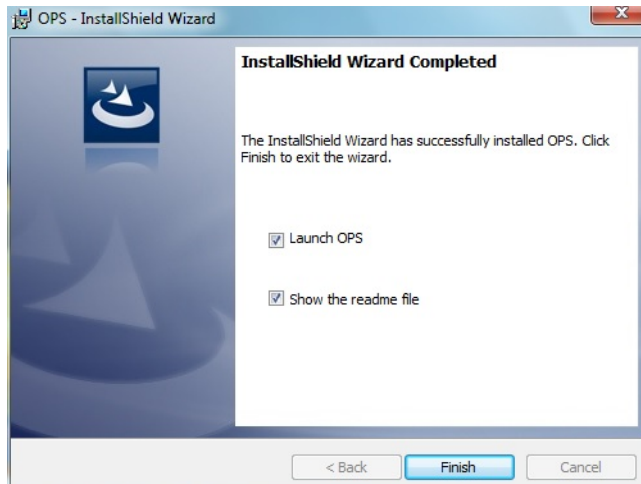
- 10 In the **Hostname** field enter either the IP or FQDN of the server on which OPS is installed. This value is the OPS server name. Make note of this value, as you will need to reference it later during device registration and HTTPS configuration.
- 11 Enter the **Passwords** in both the **OPS Details** and **DB Details** sections. Also make note of these for later use.

12 Click **Next**.The **Ready to Install the Program** screen appears.



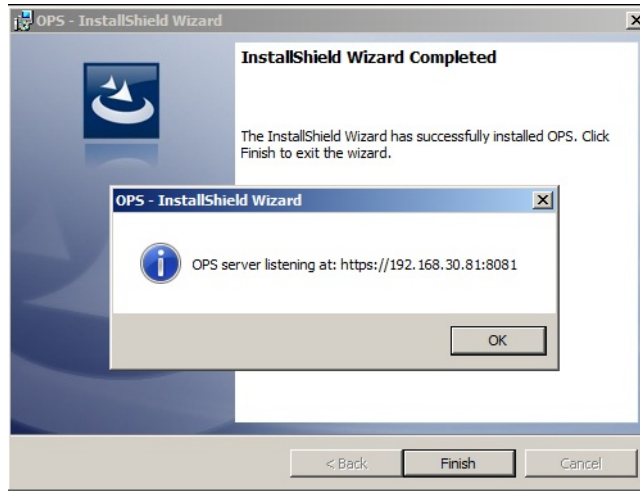
13 Click **Install**.

14 The OPS InstallShield Wizard **Completed** screen appears.

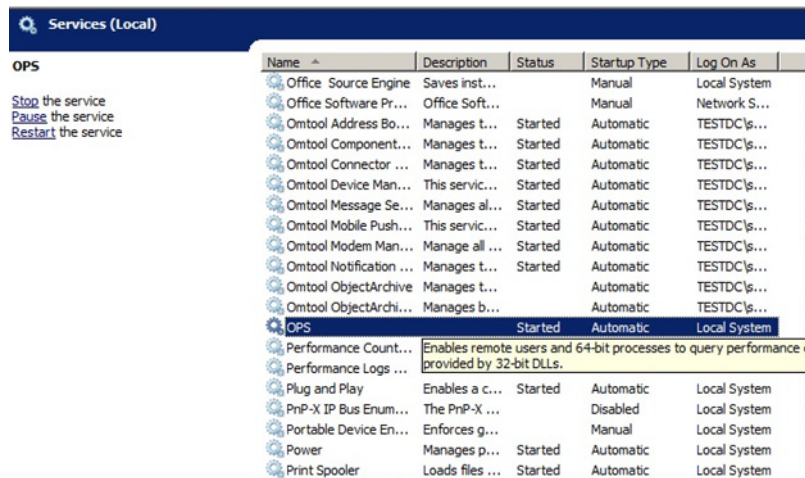


Select both the **Launch OPS** and **Show the readme file** check boxes (**Show the readme file** is optional) and then click **Finish**.

- 15 A pop-up message appears to inform you that the OPS server is listening at the IP address and port listed in step 9.



Click **OK**. **OPS** now appears as a Windows service.



Exporting the OPS server certificate

- 1 Open a Windows console and select **File > Add /Remove snap in...**
- 2 Select **Certificates** and click the **Add** button. The **Certificates** snap-in wizard appears.
- 3 Select the **Computer account** radio button and click **Next, Finish** and **OK**.
The console loads with the new **Certificate** snap-in.
- 4 Expand **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
- 5 Right-click the **OPS certificate** and select **All tasks > Export**.

- 6 The **Certificate Export** wizard appears. Select **Next**.
- 7 Choose **Base-64 encoded x.509(.CER)** and select **Next**.
- 8 Name the file and select **Browse**.
- 9 Place the certificate in `C:\Program Files (x86)\Omttool\OPS`.

Note When using the OPS-created certificate as the certificate in an HTTPS environment for HP Pro, Futuresmart and Oz devices, you must browse to place the certificate in `C:\Program Files (x86)\Omttool\DeviceClient\OPS`.

- 10 Select **Next** and then click **Finish**.

Importing the OPS certificate into the device EWS

- 1 Open and log into the EWS of the Pro Device.
- 2 On the **Network** tab select **Advanced settings > Certificates**.
- 3 Select **Import > Choose File**.
- 4 Browse to the location where the OPS certificate was saved and select **Open** and then **Finish**.

OPS registration

- 1 At a command prompt enter

```
C:\Program Files (x86)\Omttool\OPS\bin>OPSSetup
```
- 2 You will be prompted to choose from a selection of options.
Select **Option 3: Register a device to the OPS server**.
- 3 Enter the IP address for the device. For example, `123.456.78.9`.
- 4 Enter the device **username** and **password** you want to use, noted from Step 10 of [Installing the OPS kit on the remote server](#) (A-2).
- 5 Enter the **OPS server URL** you want to register. For example, `123.456.78.9:8765`.
- 6 Enter the **username** and **password** for the OPS server.

Note The OPS server URL and username can be obtained above from Steps 8 and 9 in [Installing the OPS kit on the remote server](#) (A-2). All devices will be using this Certificate for HTTPS communication.

- 7 The following message appears:

```
OPS Registered successfully
```

Your remote OPS server is now installed. See [Creating a group of devices \(part I\)](#) (6-41) for more information on creating device groups.

HTTPS support using the OPS-created certificate

Creating an SSL binding

- 1 Open the IIS Manager.
- 2 Click on the **Default Web Site** and locate **Bindings** under **Edit Site** (top right corner of the window).
- 3 Click on **Bindings**. The **Site Bindings** dialog opens.
- 4 Click on **HTTPS type** and select **Edit**. The **Edit Site Bindings** dialog opens.
- 5 In the **SSL certificate** drop-down, choose the certificate that was created earlier and click **OK**.
- 6 Click **Close** to close the dialog.

Requiring SSL for the virtual web sites

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **Device Client**.
- 3 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.
- 4 Expand **Local machine > Default Web Site** and select **WebAPI**.
- 5 Open **SSL Settings** and check **Require SLL**. Under client certificates, select **Ignore**.

Verifying the SSL binding

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 3 Click on **Browse *:443 (HTTPS)** under **Manage Application/Browse Application** (located at the top right corner of the IIS dialog). You will see this message:

There is a problem with this web site's security certificate.

Note This message is expected and safe to ignore.

- 4 Click the **Continue to this website (not recommended)** option.
- 5 Verify that the **IIS 7** dialog opens.

Enabling directory browsing in IIS

- 1 Open the IIS Manager.
- 2 Expand **Local Machine > Default Web Site** and select **DeviceClient**.
- 3 Double-click on **Directory browsing**.
- 4 In the right **Actions** field, select **ENABLE**.
- 5 Expand **Local Machine > Default Web Site** and select **WebAPI**.

- 6 Double-click on **Directory browsing**.
- 7 In the right **Actions** field, select **ENABLE**.

Verifying HTTPS browsing

- 1 Open the IIS Manager.
- 2 Expand the **Default Web Site**.
- 3 Expand **OWS**.
- 4 Select the **Configuration** folder.
- 5 In the actions pane, select **Browse*:443(https)**.
- 6 Select **Continue to this website (not recommended)**.
- 7 Verify that the local page is displayed:
`.../DeviceClient/Configuration/`
- 8 In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
- 9 In the actions pane, select **Browse*:443(https)**.
- 10 Select **Continue to this website (not recommended)**.
- 11 Verify that the localhost page is displayed:
`.../WebAPI/`
- 12 Select **Continue to this website (not recommended)**.

Editing the OmISAPIU.xml file

- 1 Navigate to the following path.
`C:\Program Files (x86)\Omtool\OmtoolServer\WebAPI\WebAPI\Scripts`
- 2 In `OmISAPIU.xml`, find the FileTransfer node. Replace the IP address with the OPS Servername or IP. Also, change `http` to `https`.
`<FileTransfer>https://OPS Servername or IP/WebAPI/FileTransfer/
</FileTransfer>`
- 3 This OPS Servername is based on the value noted from Step 10 of [Installing the OPS kit on the remote server \(A-2\)](#).

Note XML files can be edited using Microsoft Notepad.

- 4 Save the file.

Editing the Bootstrap.xml file

- 1 Navigate to the following path.
`C:\Program Files (x86)\Omtool\DeviceClient\Configuration`

- 2** In bootstrap.xml, change `http` to `https`.

```
<Server>https://OPS Servername or IP/webapi/scripts/omisapiu.dll </
Server>
```

- 3** This OPS Servername is based on the value from noted from Step 10 of [Installing the OPS kit on the remote server](#) (A-2).

|

Appendix B: Installing Buttons on HP S900 Series MFP Devices

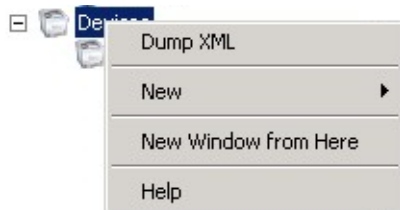
This appendix describes the processes for

- [Adding buttons to HP S900 Series MFP devices](#) (B-1)
- [Device authentication](#) (B-3)

Adding buttons to HP S900 Series MFP devices

Note It is recommended that you install the buttons as Nested buttons. For more information, see [Using Nested buttons](#) (B-2).

- 1 In the HP CR MMC Administrator, acquire an **XML Group Dump** from the Device Group. Highlight the **Devices** node, right-click on it while holding the CTRL key and select **Dump XML**. By default, this .xml opens in Internet Explorer.



- 2 In a browser, open the **Embedded Web Server** for the HP S900 Series device by entering the IP address of the device, and log in.
- 3 From the left menu, select **Application Settings/External Application Settings**.
- 4 Select **Add(Y)**.
- 5 In the **Standard Application Registration** page, add an **Application Name** for the feature button.
- 6 In **Address for Application UI**, use the following generic URL string:
http://DeviceClientServerIP/Device_Client/device.aspx?Group=<GroupName>&FeatureID=<FeatureID>&ClearHistory=1
- 7 Replace the following fields with the appropriate values:
 - ▶ **Device Client Server IP**
 - ▶ **Group name**

► Feature ID

You can find the **Group name** under **Devices** in the Server Administrator.

Copy the **Feature ID** value from the **Dump XML** `<Feature id= >`. This corresponds with the Feature Button created in the HP CR Administrator.

Note If there are multiple Device Groups, verify the Group Node before searching for the feature button.

- 8 The following XML Group dump example shows a Nested button `feature id` within the HP S900 Series Device Group:

```

</UI>
</Additional/>
</Confirmation/>
</DeliveryConfirmations/>
<FeatureSets>
- <shuttle_918177c4574242e0b301c2d269b3b8de>
  - <Feature id="Button0" enabled="true" toplevel="true" type="Button">
    <Image/>
    <Text>HP Capture & Route</Text>
    <Description>Scan to HP Capture and Route</Description>
    <AllowJobBuild>false</AllowJobBuild>
    <EnablePreview>false</EnablePreview>
    <AllowUseByNonAuthenticatedUsers>true</AllowUseByNonAuthenticatedUsers>
    <CaptureAuthenticatedPassword>false</CaptureAuthenticatedPassword>
    <CaptureAuthenticatedPasswordAlwaysPrompt>false</CaptureAuthenticatedPasswordAlwaysPrompt>
  - <FeatureSpecific>
    <GUID>c9e9e27e-8d07-47c0-8de3-4ddacac029cc</GUID>
    <priority>1</priority>
    <help>@helpfeatures</help>
    <ImageNormal>nested</ImageNormal>
    <PersonalED1/>
    <RoutingSheet2/>
    <GroupED3/>
    <MyAccuRoute4/>
    <ScanToDataProvider5/>
    <Fax6/>
  </FeatureSpecific>
</Feature>
- <Feature id="PersonalED1" enabled="true" toplevel="false" type="PersonalED">
  <Image/>
  <Text>@buttonpersonalText</Text>
  <Description>@buttonpersonalDesc</Description>
  <AllowJobBuild>false</AllowJobBuild>
  <EnablePreview>false</EnablePreview>
  <AllowUseByNonAuthenticatedUsers>false</AllowUseByNonAuthenticatedUsers>
  <CaptureAuthenticatedPassword>false</CaptureAuthenticatedPassword>
  <CaptureAuthenticatedPasswordAlwaysPromnt>false</CaptureAuthenticatedPasswordAlwaysPromnt>

```

In this example, the specific string created is

```
http://10.0.0.1/DeviceClient/
device.aspx?Group=hp&FeatureID=Button0&ClearHistory=1
```

Using Nested buttons

It is recommended that you use Nested buttons, because:

- The HP S900 Series MFP devices have a display limit of 8 buttons in the main window.
- Nested buttons need only be registered once, as opposed to the individual registrations required if they were not nested.

For more information about Nested buttons, see [AccuRoute scanning features in AccuRoute Embedded Device Client](#) (1-2).

Device authentication

- 1 In a browser, open the **Embedded Web Server** for the device and log in.
- 2 Select **Network Settings > LDAP settings**.
- 3 Enter the **Name**, **Search root**, and **LDAP server IP** information.
- 4 Set **Server Type** to **Custom** (the Search attribute has a default value of **CN**.)
- 5 Optionally, you can set other **Custom Attributes**, which allow for additional return results.
- 6 Enter the **Domain\Username** and **Password** for LDAP queries.
- 7 Change the **Bind Prefix** to **CN**. This will search based on the user's Common name and can be changed to any Active Directory Attribute.

Note Other login options are available based on Email address or User number.

- 8 Select **Execute** to verify LDAP search permissions and then select **Submit**.
- 9 From the left menu, select **User Control > Default Settings**.
- 10 Select **User Authentication > Enable**.
- 11 Select **Authentication Method Setting > Authenticate a User by Login name and Password**.
- 12 Select **Submit** and then **Update**.

Appendix B: Installing Buttons on HP S900 Series MFP Devices